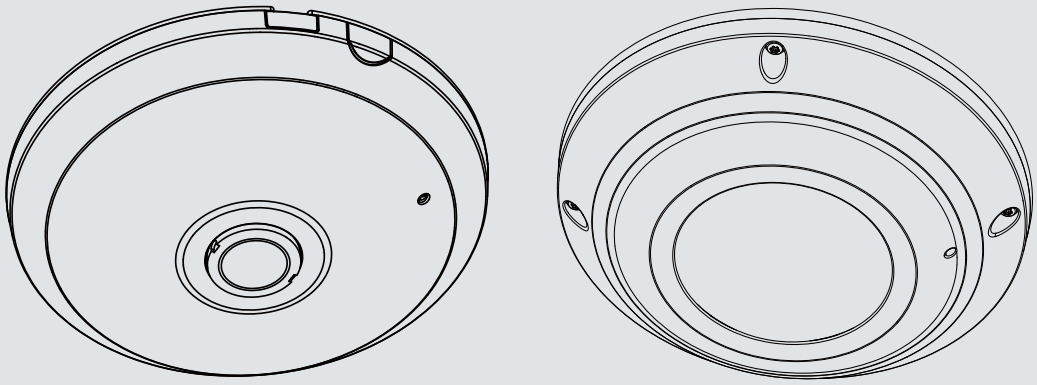
VIVOTEK

# SF8172/8172V Fixed Dome Network Camera

# User's Manual

**5MP • 360º Surround View • IP66 • Vandal Proof**



Rev. 1.0

SUPREME

# Table of Contents


*Overview* ..... *4*

Read Before Use ..... 5
Package Contents ..... 5
Symbols and Statements in this Document ..... 5
Physical Description - SF8172V ..... 6
Physical Description - SF8172 ..... 8
Hardware Installation - SF8172V ..... 10
Hardware Installation - SF8172 ..... 13

*Network Deployment* ..... *22*

Setting up the Network Camera over the Internet ..... 22
Software Installation ..... 25
Ready to Use ..... 26

*Accessing the Network Camera* ..... *27*

Using Web Browsers ..... 27
Using RTSP Players ..... 30
Using 3GPP-compatible Mobile Devices ..... 31
Using VIVOTEK Recording Software ..... 32

*Main Page* ..... *33*
*Client Settings* ..... *43*

H.264 / MPEG-4 Media Options ..... 43
H.264 / MPEG-4 Protocol Options ..... 43
MP4 Saving Options ..... 44
Local Streaming Buffer Time ..... 44

*Configuration* ..... *45*

System > General settings ..... 46
System > Homepage layout ..... 48
System > Logs ..... 51
System > Parameters ..... 52
System > Maintenance ..... 53
Media > Image ..... 57
General settings ..... 57
Day/Night Settings ..... 58
Image settings ..... 59
Exposure ..... 62
Privacy mask ..... 65
Pixel calculator ..... 66
Media > Video ..... 67
FOV ..... 67
Stream settings ..... 68
Media > Audio ..... 72
Audio Settings ..... 72

Network > General settings ..... 73
Network > Streaming protocols ..... 81
Network > QoS (Quality of Service) ..... 86
Network > DDNS ..... 88
Manual setup ..... 89
Network > SNMP (Simple Network Management Protocol) ..... 91
Security > User Account ..... 92
Security > HTTPS (Hypertext Transfer Protocol over SSL) ..... 93
Security > Access List ..... 100
Security > IEEE 802.1x ..... 103
PTZ > PTZ settings ..... 105
Digital PTZ Operation (E-PTZ Operation) ..... 105
Event > Event settings ..... 108
Event ..... 108
Add server ..... 111
Add media ..... 115
Applications > Motion detection ..... 121
Applications > DI and DO ..... 124
Applications > Tampering detection ..... 124
Applications > Panoramic PTZ ..... 125
Recording > Recording settings ..... 131
Local storage > SD card management ..... 136
SD card staus ..... 136
SD card control ..... 136
Local storage > Content management ..... 137
Searching and Viewing the Records ..... 137
Search Results ..... 138

*Appendix ..... 140*

URL Commands for the Network Camera ..... 140
1. Overview ..... 140
2. Style Convention ..... 140
Technical Specifications ..... 232
Technology License Notice ..... 233
MPEG-4 AAC Technology ..... 233
MPEG-4 Visual Technology ..... 233
AMR-NB Standard ..... 233
Electromagnetic Compatibility (EMC) ..... 234

# Overview

VIVOTEK SF8172/72V are the latest fisheye fixed dome network cameras from VIVOTEK, featuring a detailed 5-Megapixel resolution sensor with superb image quality. Equipped with a fisheye lens for 360° surround view (ceiling/floor/table mount) without blind spots, the camera is able to provide coverage of wide, open areas, such as airports, shopping malls, parking lots, retail stores, offices and more.

As with all VIVOTEK true day/night cameras, the SF8172/72V feature removable IR-cut filters, maintaining clear images 24 hours a day. SF8172V's IP66-rated housing is designed to help the camera body withstand rain and dust and ensures operation under a multitude of harsh weather conditions; additionally, the vandal-proof IK10-rated housing effectively provides robust protection from physical damage. Together with 802.3af compliant PoE, MicroSD/SDHC/SDXC card slot for on-board storage, EN50155 (SF8172V only) and iPad applications, the SF8172/72V are indisputably the top choice for constructing a robust surveillance system with the greatest coverage possible.

Moreover, SF8172/72V are compatible with the VIVOTEK Panoramic PTZ solution. Panoramic PTZ is a groundbreaking new technology developed by VIVOTEK for monitoring open areas with extreme detail. This feature is realized through the synergy of a VIVOTEK megapixel fisheye camera with speed dome camera, and allows users to simultaneously monitor an area overview from a fisheye model while providing the capability for a detailed regional view from a speed dome.  Suitable applications for Panoramic PTZ include department stores, station lobbies, airports, parking lots, and any wide open areas where comprehensive video surveillance systems and the capability for extreme video detail are essential.

## Revision History

Rev. 1.0: Initial release. These models are to be configured into a Panoramic PTZ configuration.

## Read Before Use

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but can also be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the Package Contents listed below. Take note of the warnings in the Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damage due to faulty assembly and installation. This also ensures the product is used properly as intended.

The Network Camera is a network device and its use should be straightforward for those who have basic networking knowledge. It is designed for various applications including video sharing, general security/ surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For creative and professional developers, the URL Commands of the Network Camera section serves as a helpful reference to customizing existing homepages or integrating with the current web server.

## Package Contents

- SF8172V or SF8172 Camera
- Mounting plate (SF8172V)/ Screwdriver
- Alignment Stickers (for mounting plate and for camera base)
- Screws / Anchors / Desiccant Bag / Double-sided tape/ Rubber seal plug / Rubber washer (SF8172V)
- Screws, anchors, cable ties (SF8172)
- Power & I/O Cables
- Quick Installation Guide / Warranty Card
- Software CD

## Symbols and Statements in this Document

**INFORMATION:** provides important messages or advices that might help prevent inconvenient or problem situations.

**NOTE**: Notices provide guidance or advices that are related to the functional integrity of the machine.

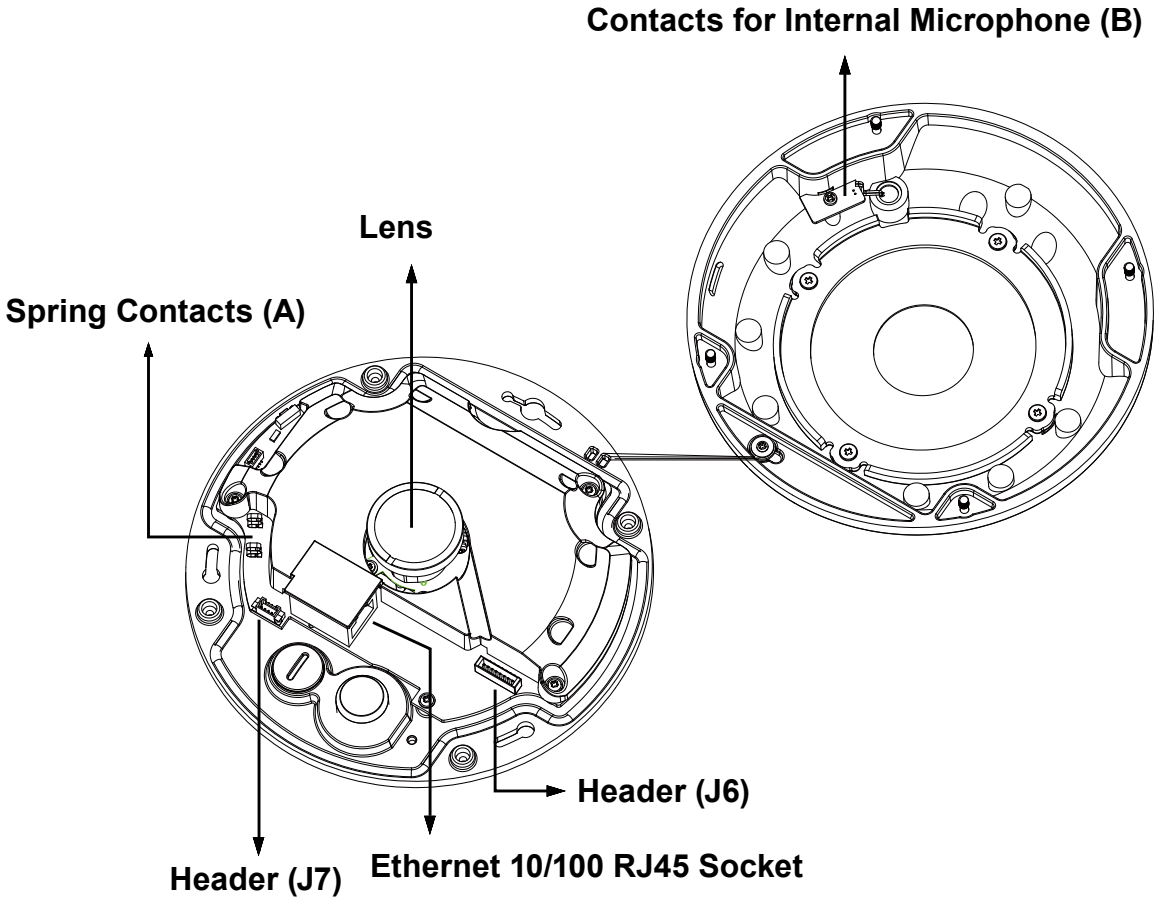
**Tips**: Tips are useful information that helps enhance or facilitae an installation, function, or process.

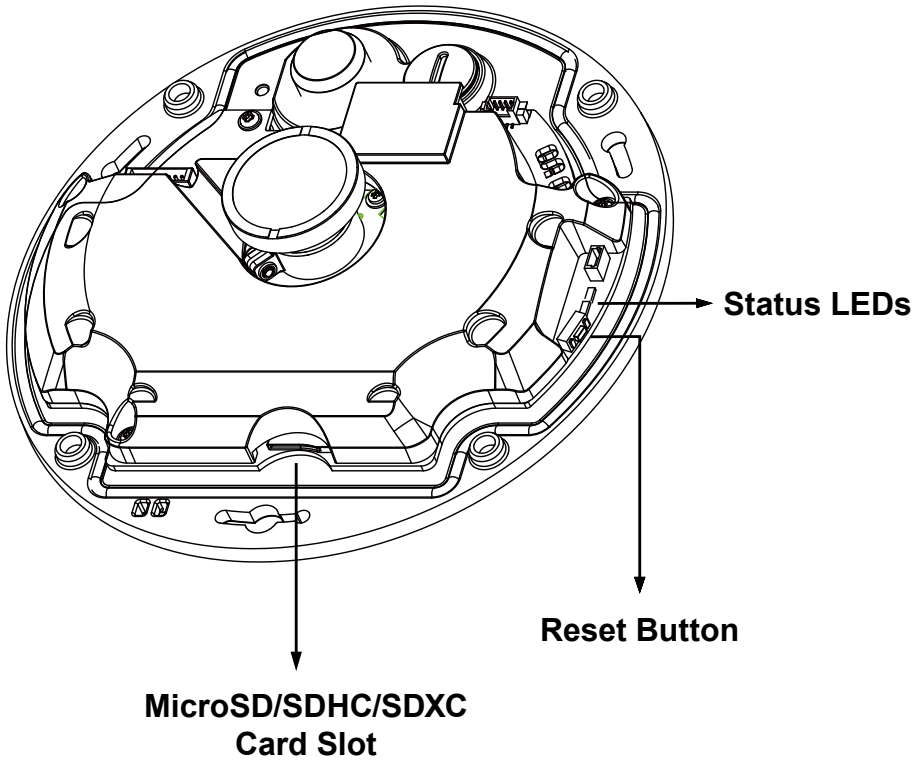
**WARNING! or IMPORTANT!**: These statements indicate situations that can be dangerous or hazardous to the machine or you.

**Electrical Hazard**: This statement appears when high voltage electrical hazards might occur to an operator.

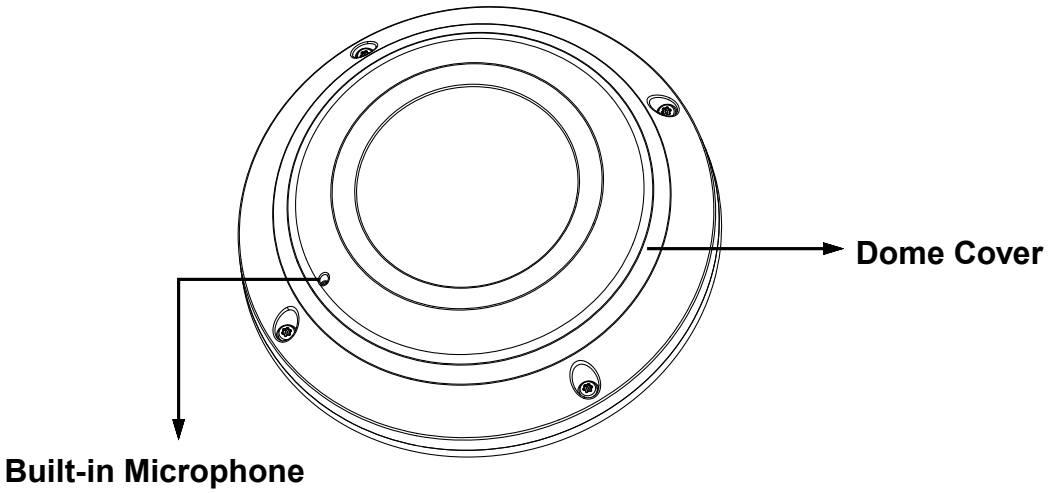
# Physical Description - SF8172V

**Inner View**



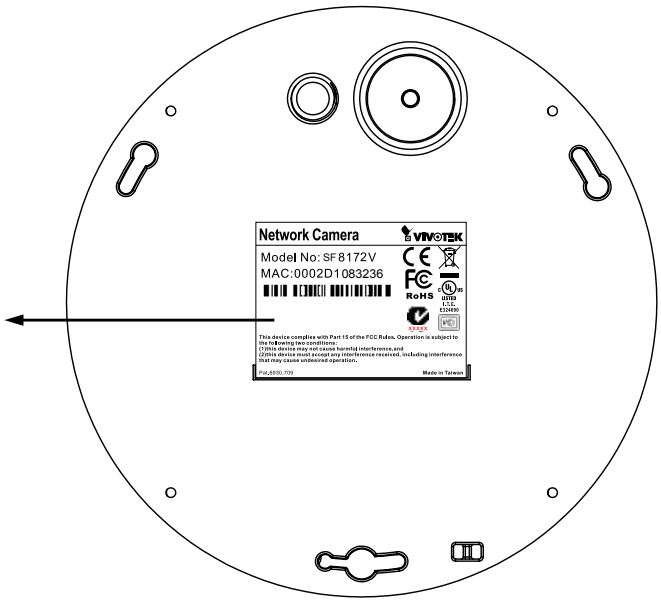



## Outer View



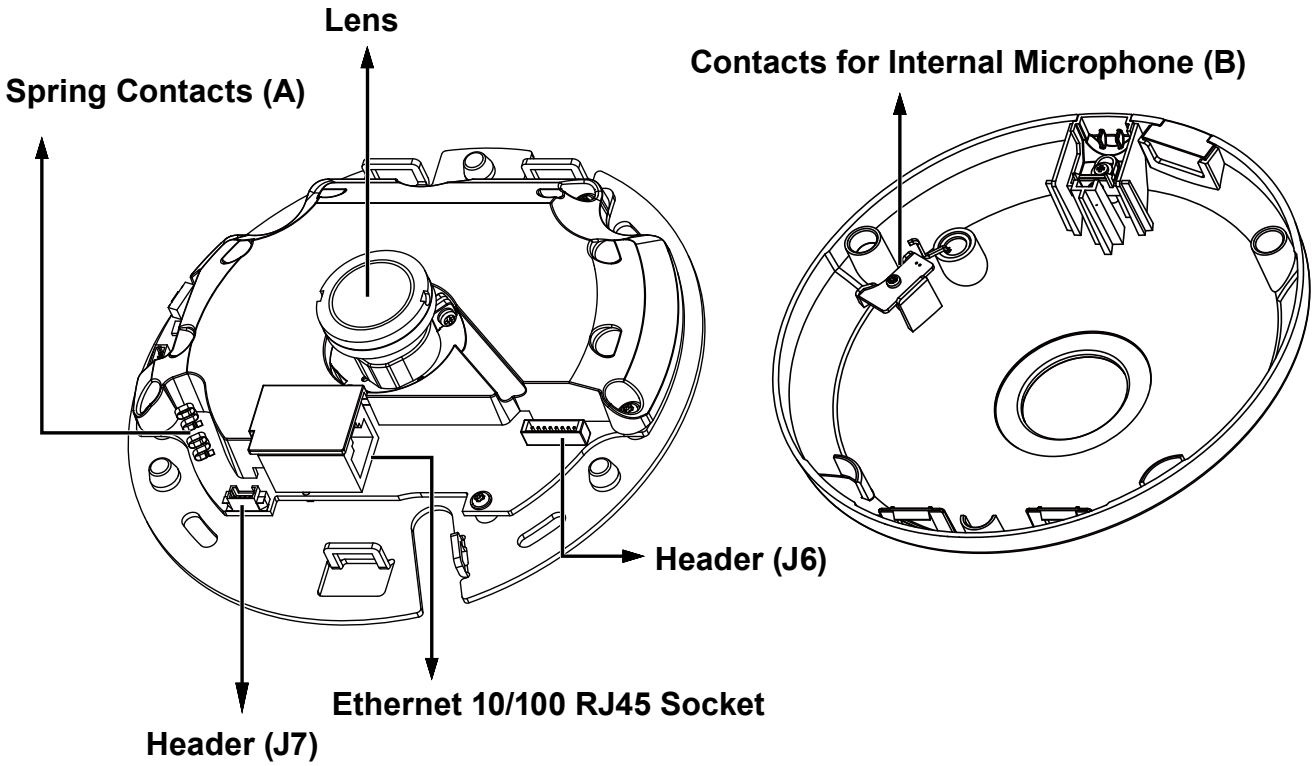

**IMPORTANT:**

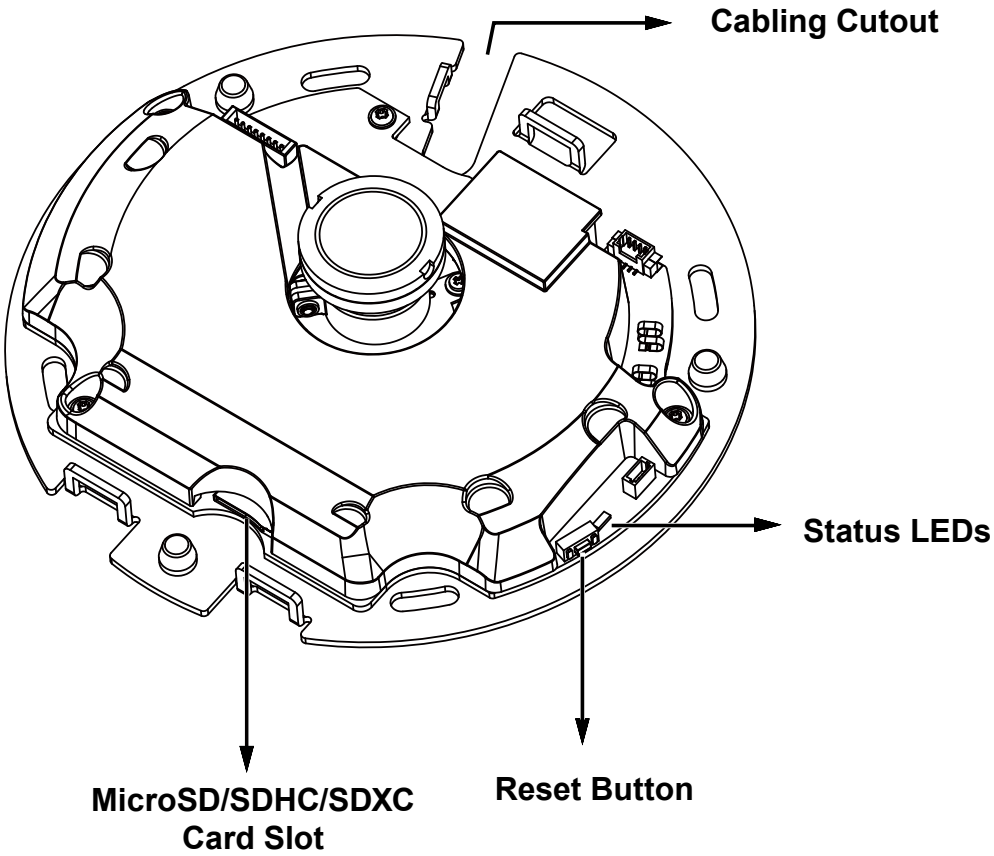
Record the MAC address under the camera base before installing the camera.



# Physical Description - SF8172

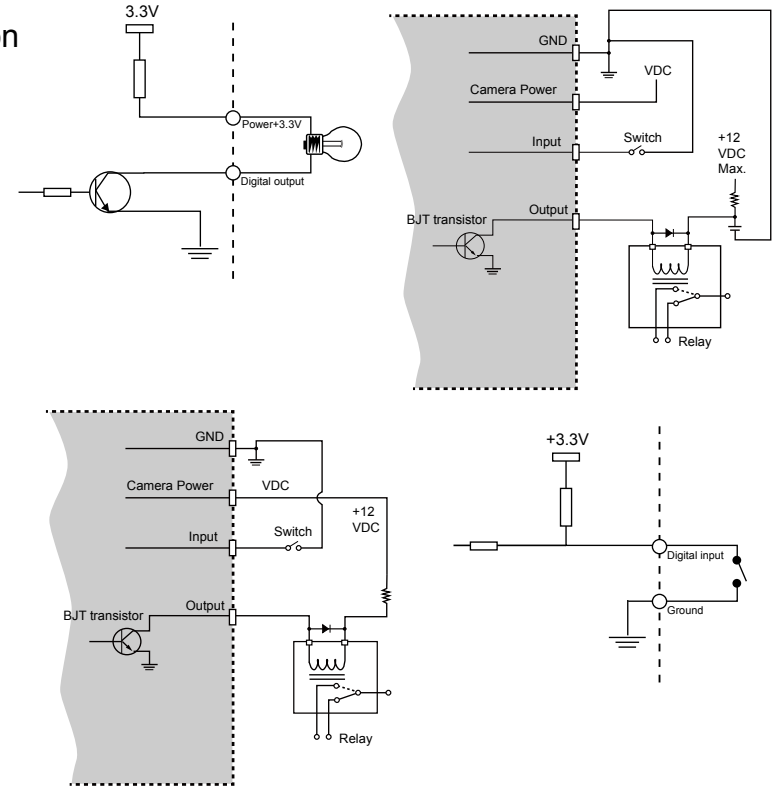
## Inner View



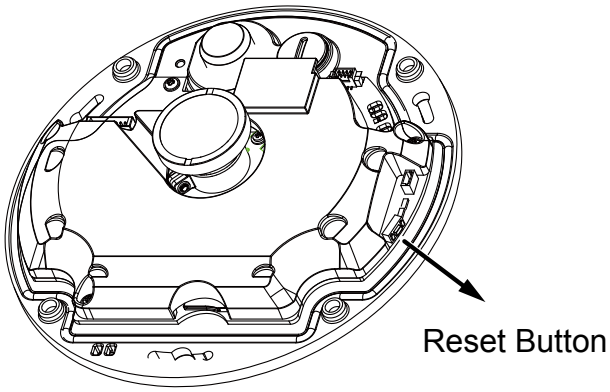



## DI/DO Diagram

Please refer to the following illustration for the connection method.




## Hardware Reset




The reset button is used to reset the system or restore the factory default settings. Sometimes resetting the system can return the camera to normal operation. If the system problems remain after reset, press the reset button longer to restore the factory settings and install again.

Reset: Press and release the recessed reset button with a straightened paper clip. Wait for the Network Camera to reboot.

Restore: Press and hold the recessed reset button for at least several seconds to restore. Note that all settings will be restored to factory defaults.

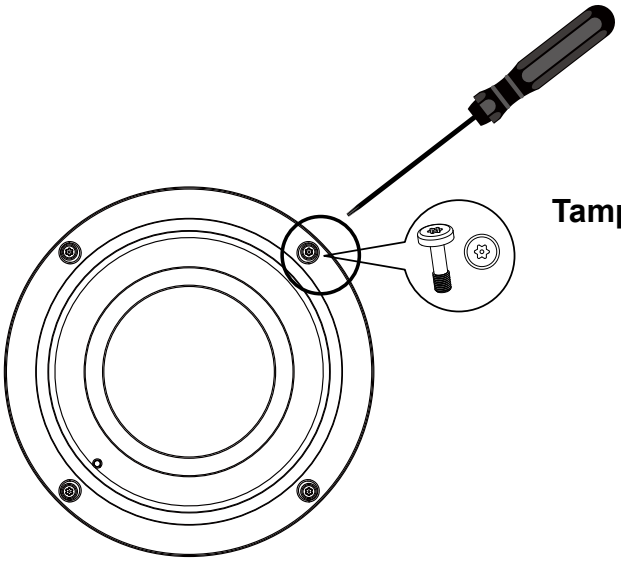
## Micro SD/SDHC/SDXC Card Capacity

This network camera is compliant with **Micro SD/SDHC 32GB** and other preceding standard SD cards.

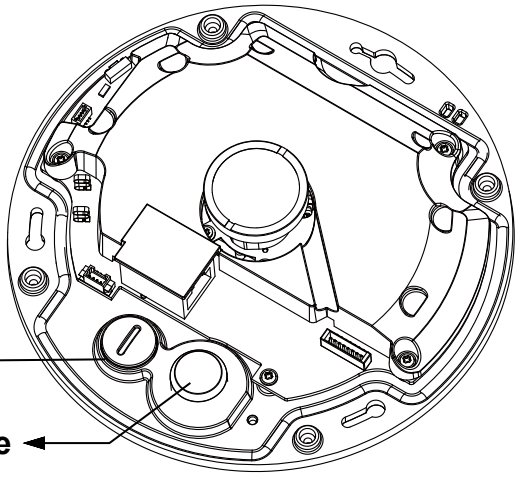
# Hardware Installation - SF8172V

## Opening Dome Cover

First, use the supplied screwdriver to loosen the four screws and detach the dome cover from the camera base. Then, follow the steps below to install the camera to either a ceiling or a wall.



**Tamper-proof Screw**



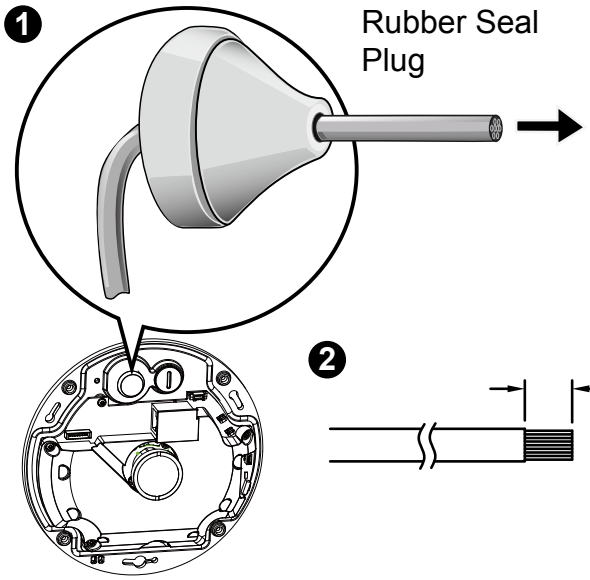
Remove the stoppers and route cables through the openings.

**Rubber Stopper on the hole for Power & IO Cables**

**Rubber Seal Plug on the hole for RJ45 Ethernet Cable**

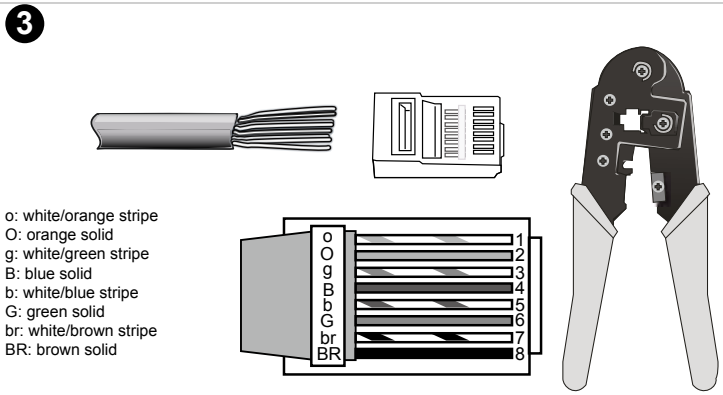
## Connecting RJ45 Ethernet Cable

**Assembly Steps**

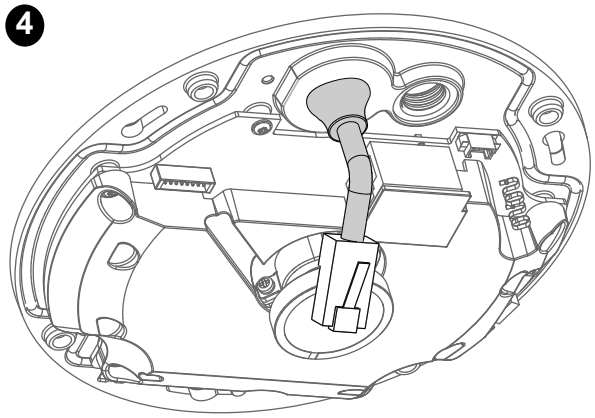



1. Drill a hole on the rubber seal plug and insert an Ethernet cable through the opening.

2. Strip part of the sheath from the Ethernet cable.



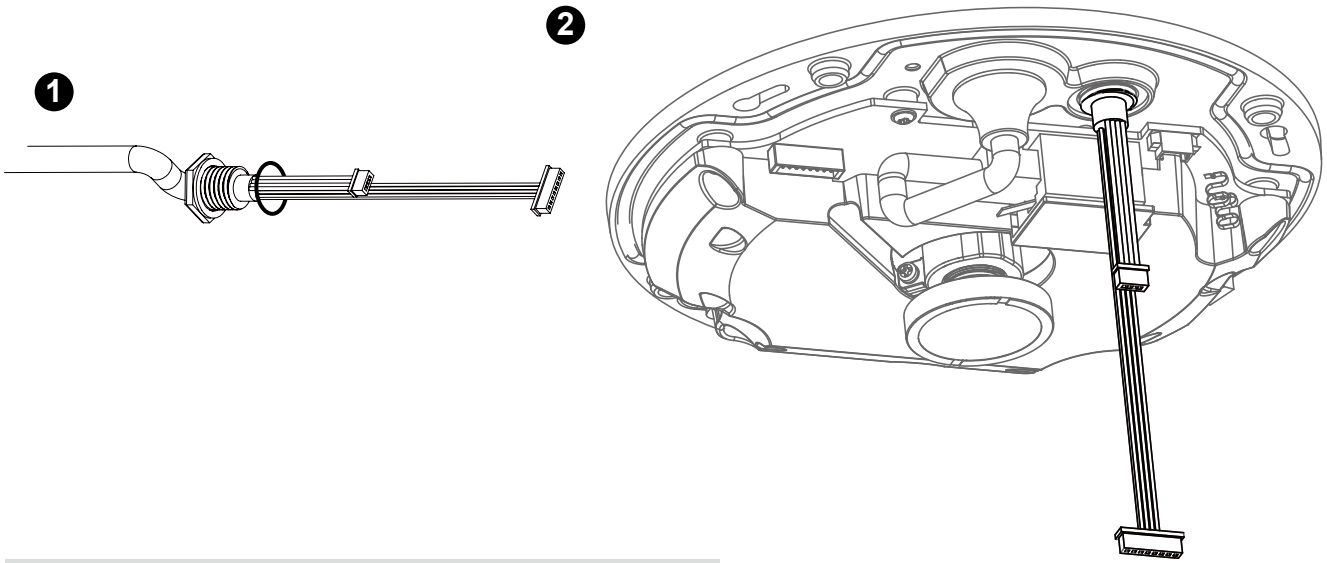

3. You will need an RJ45 crimping tool to attach the Ethernet wires to a connector. When done, connect the cable to the camera's Ethernet RJ45 socket.



4. Feed the Ethernet cable from the bottom of the camera and through the hole. Attach the rubber seal plug for water proofing.

## Connecting DC Power Cable

1. Add the supplied rubber washer to the cable as shown in the picture.
2. Feed the cable from the bottom of the camera and tighten the plastic base for waterproofing.



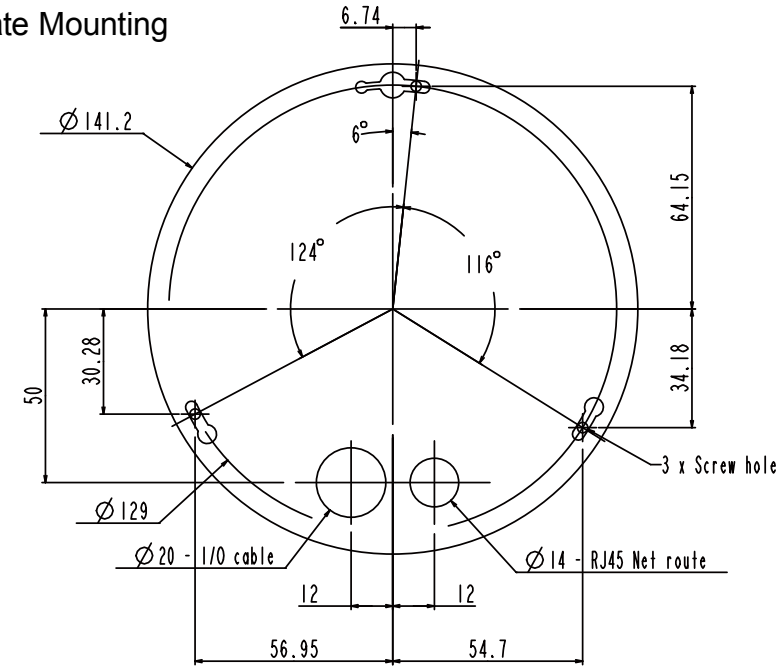
**NOTE:**

Connect the supplied power & IO cables if your switch does not support PoE.

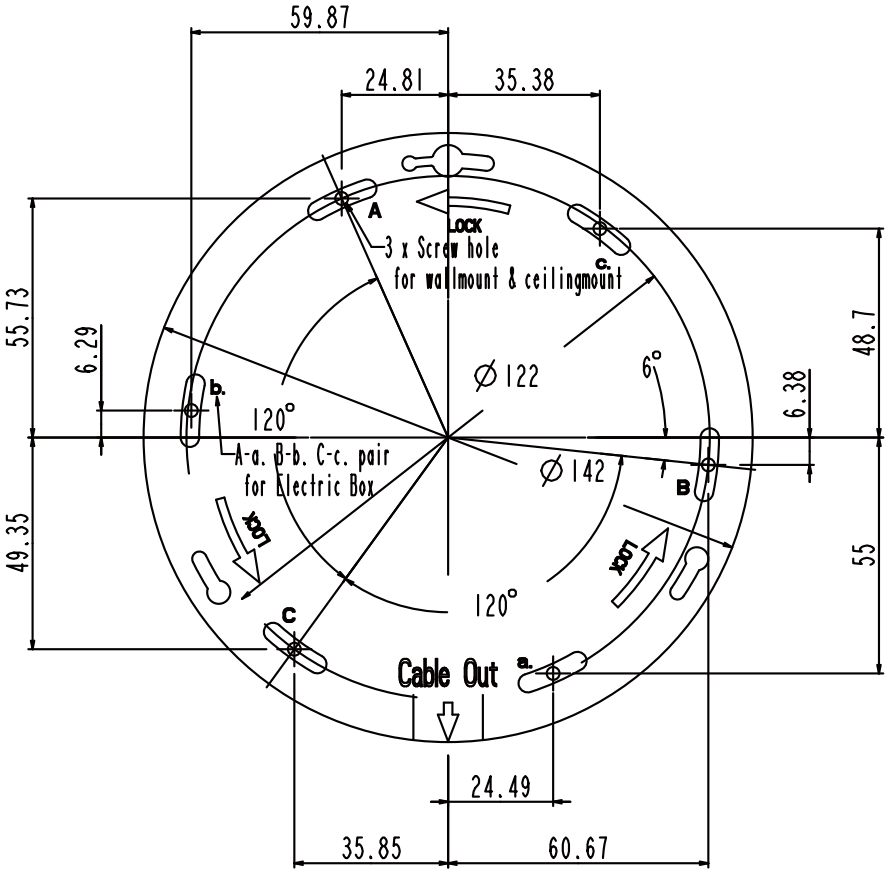
## Base Plate Mouting Positions

Refer to the diagram on the right for the mounting hole positions and the dimensions of the base plate.

Camera Base Plate Mounting Positions

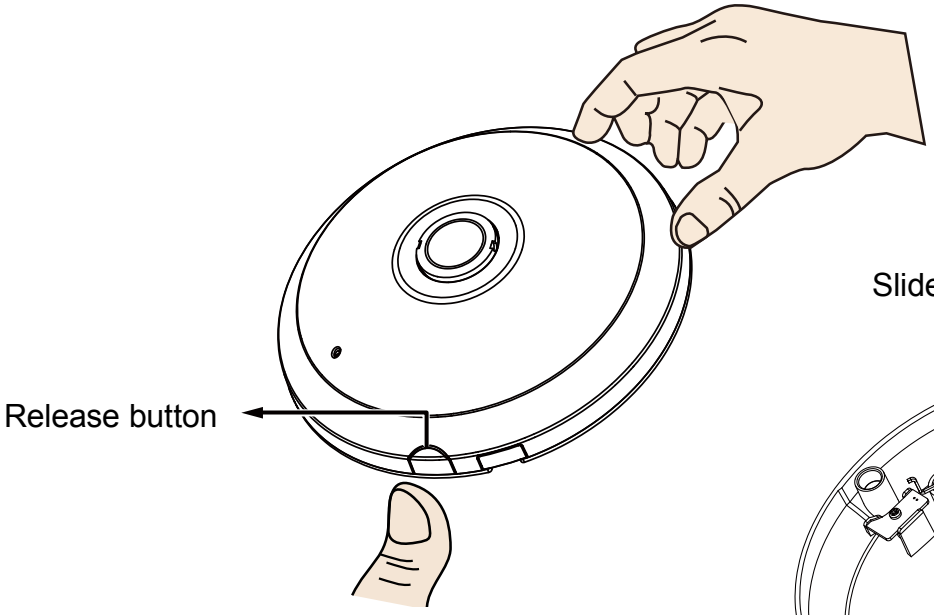


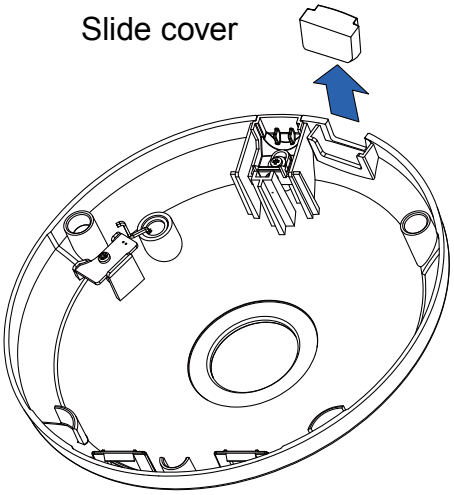

Camera Mounting Plate Mounting Positions - SF8172V



# Hardware Installation - SF8172

First, open the dome cover by pressing the release button. You may squeeze the opposite edge of the dome cover if the dome cover does not come off easily. Then, follow the steps below to install the camera to either a ceiling or a wall.

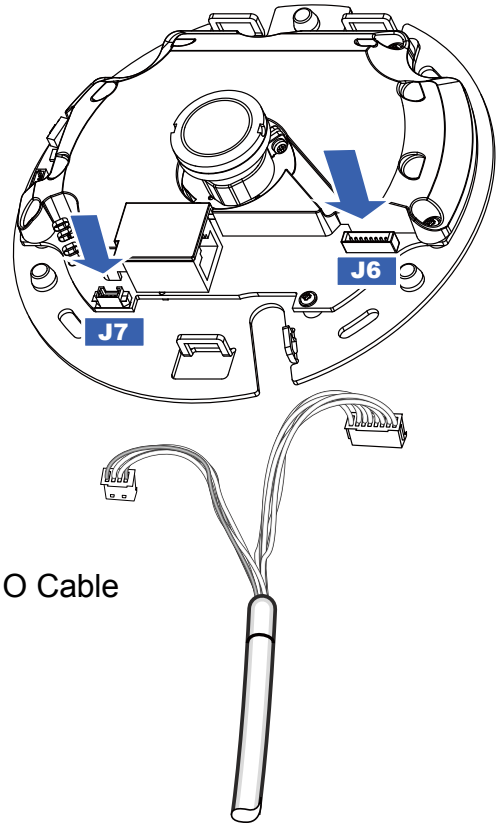



If you plan to route cables from the side of camera, remove the rubber slide cover from the dome cover.

**Connecting Ethernet Cable & the Power and IO Cable**

Connect the supplied power & IO cables if your switch does not support PoE. Connect the white header connectors to J6 and J7 on the camera.

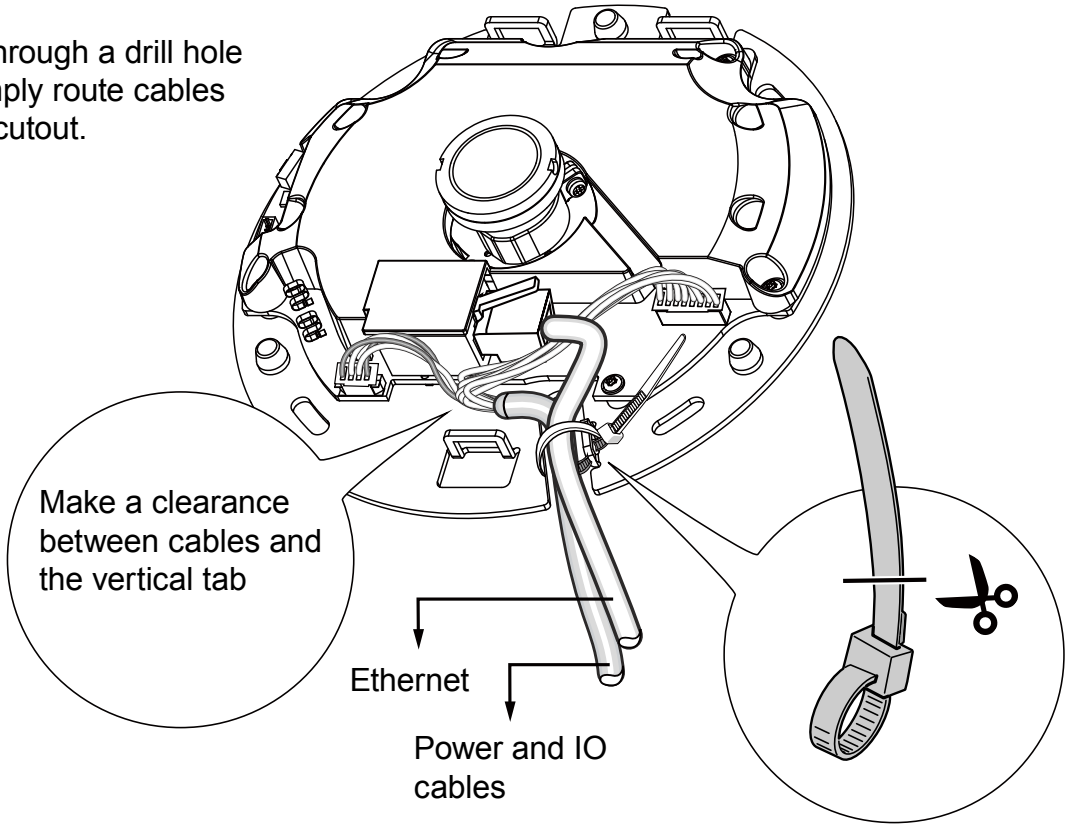


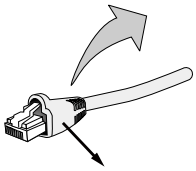
## Connecting Cables

If you need to route cables through the side opening, proceed with the following:

1. Connect the Ethernet and the Power & IO cables. The Ethernet cable is user-supplied.
2. Use an included cable tie to secure the Ethernet and IO cable to the base plate. Insert the cable tie through the vertical mounting tab located on the edge of the cabling cutout.
3. Make a clearance between cables and the vertical mounting tab. Arrange the cables neatly to avoid getting in the way when the dome cover is attached.
4. Cut the extra length from the cable tie.

If you route cables through a drill hole on a wall/ceiling, simply route cables through the cabling cutout.



Strain relief boot

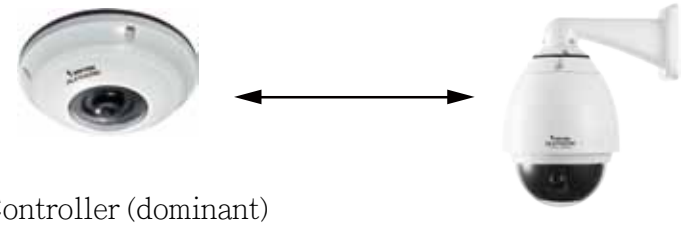
It is recommended to remove the strain relief boot if your Ethernet cable comes with one.

**IMPORTANT for both SF8172V and SF8172:**

Refer to the "**Panoramic PTZ Installation Guide**" in your product CD for design considerations before you proceed with physical installation.

The camera is intended to be installed with an SD series speed dome camera in a "Panoramic PTZ" configuration. Users should take the following into account:

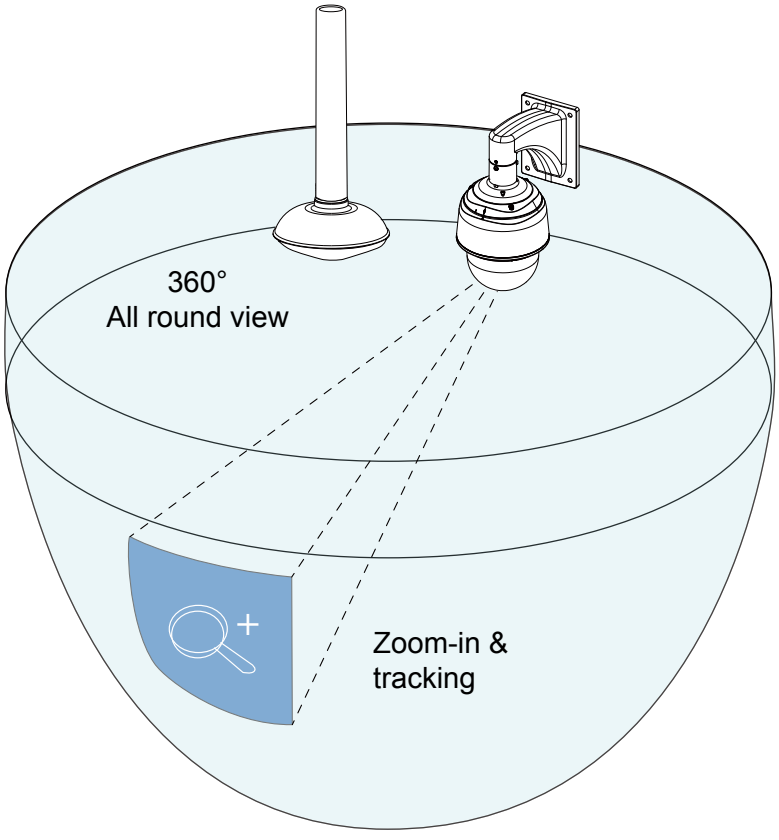
1. There is a dominant - subordinate relationship between the fisheye camera and the speed dome. All configurations are done on a PC running the Calibration tool and a web console with the fisheye camera. The computation required for exerting the Panoramic PTZ control takes place on the fisheye camera.



Controller (dominant) camera

Auxiliary (subordinate) camera

2. In a panoramic PTZ configuration, the fisheye camera provides an overview over the 360° hemispheric field of view; while the speed dome provides tracking, zooming, and keeping an object in a view of an adequate size. The configuration is operated via the VAST or Milestone software with easy clicks and drags.

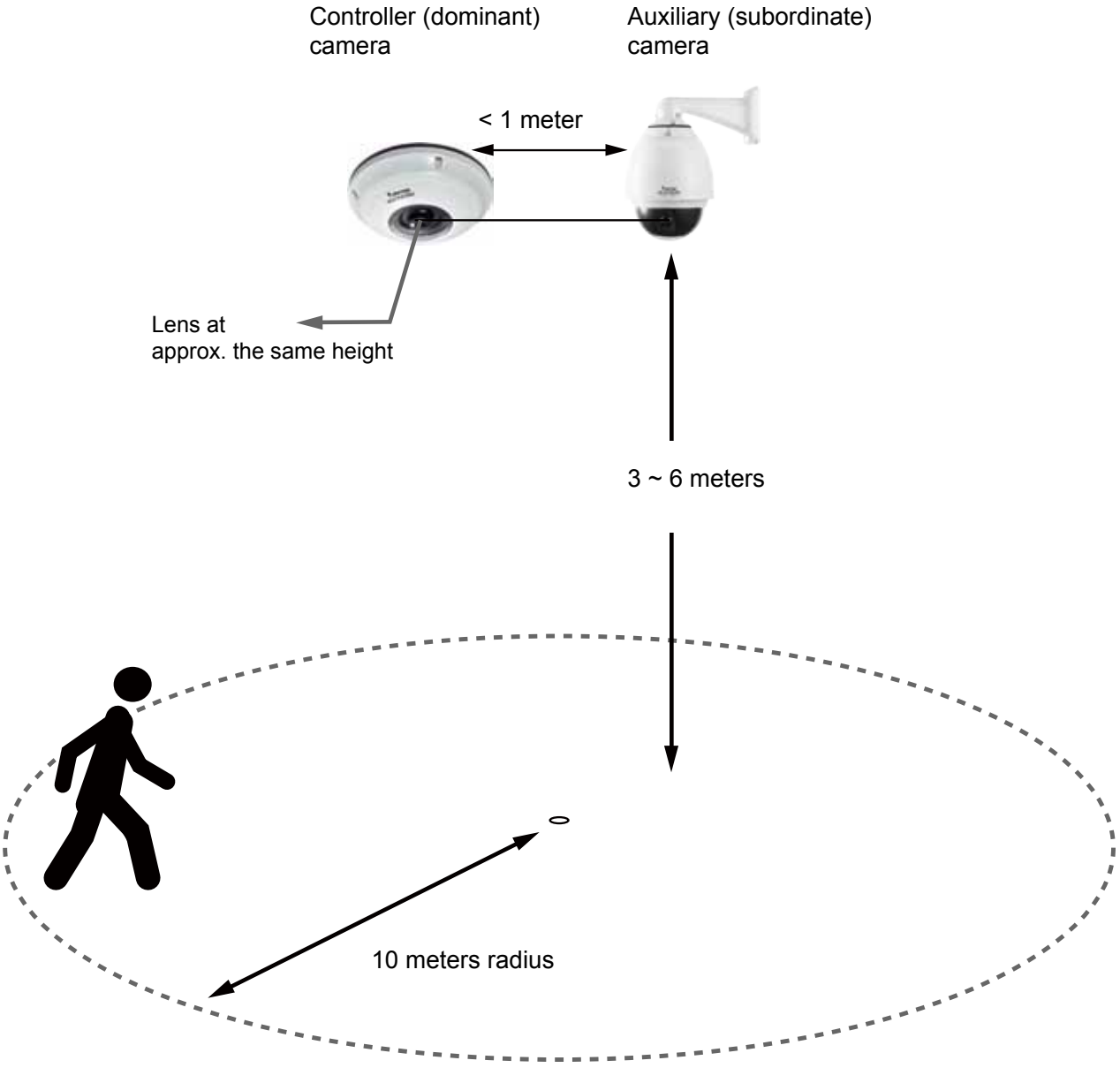


## Installation Concerns

Note the following when installing the fisheye and speed dome cameras:

1. Mount the cameras closely together, no greater than **1** meter apart.
2. The cameras should be mounted at the height of **3** to **6** meters from the ground, and their lens at approximately the same height.
3. A configuration thus configured can cover a surveillance area of a radius of **10** meters*.
4. Auto tracking, if applied, is designed to track an intruder in a place where human traffic is not heavy, such as a warehouse or a load area. Heavy traffic can result in a constant shift of tracked objects, and reduce the effectiveness of the feature.

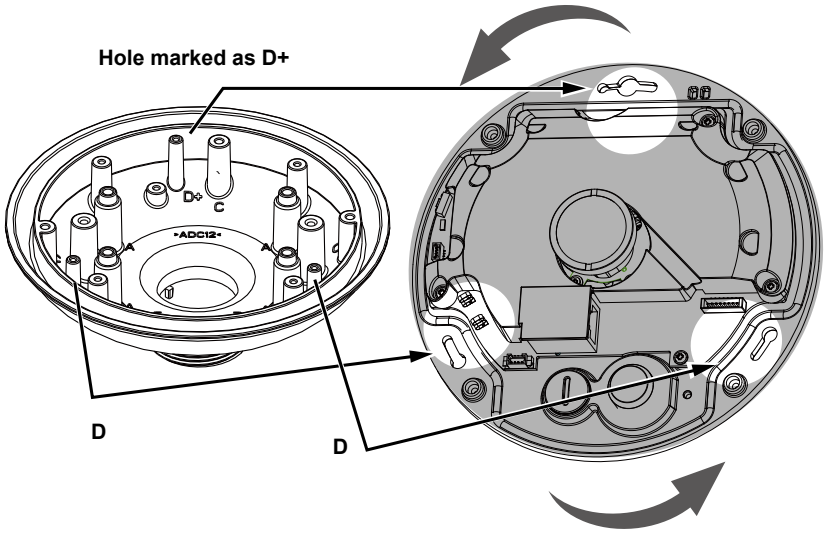
* Note that the 10 meter radius area only applies when using the Auto tracking feature. If using manual control, the surveillance area can be much larger.



## Attach Camera to Mounting Adaptor - SF8172V

To attach the camera to AM-51A mounting adaptor,

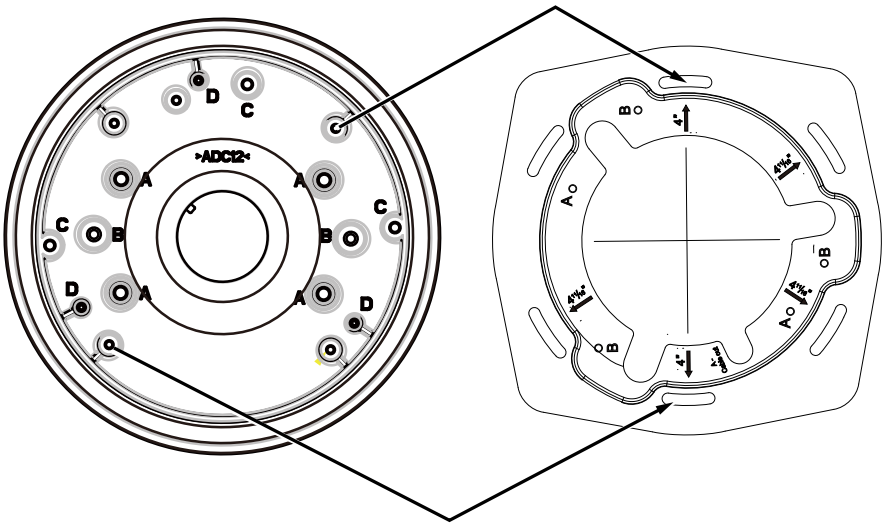
1. Remove the camera's top cover.
2. Fasten 2 included screws to the D holes (not the D+ hole).
3. Route cables through the adaptor.
4. Align the camera with the mounting adapter and let the 2 screws enter the key holes located on the sides where the camera's cabling interfaces reside, e.g., the Ethernet port.
5. Rotate the camera counter-clockwise. You can then see the D+ hole through the slotted screw hole (in front of the Micro SD slot).
6. Fasten screws to secure the camera to the mounting adapter.



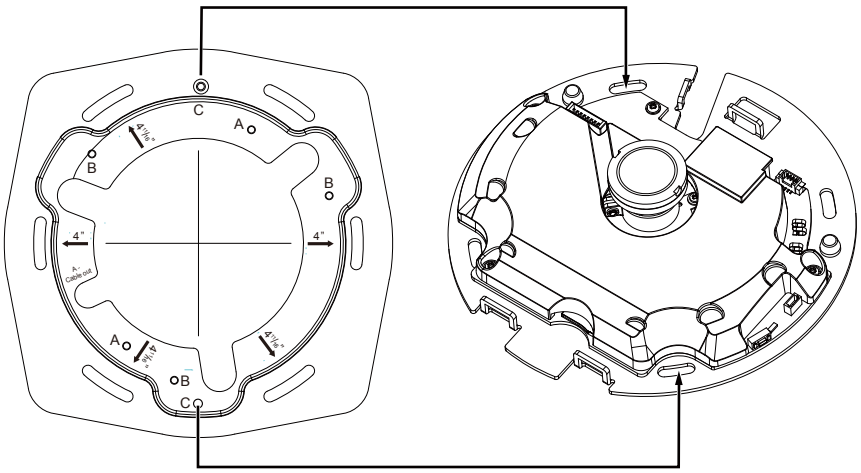

## Attach Camera to Mounting Adaptor - SF8172

An adapter bracket, AM-517, is required.

1. Align the bracket's screw slots with mounting holes on the AM-51A.
2. Secure the bracket to AM-51A using 2 pan head M2.6 screws.



3. Align the camera's screw slots with the C holes.
4. Use the included M2.6 screws to secure camera to bracket.




**NOTE:**

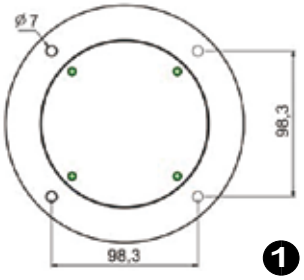
The following procedure applies to both SF8172V and SF8172 except that the SF8172 has a plastic dome cover.

## Ceiling Mount Installation

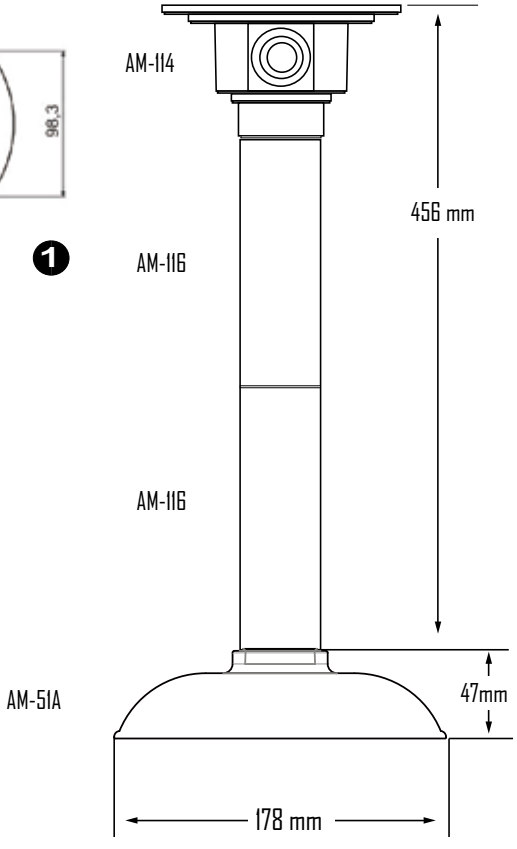
Install the Pendant Pipe

Below is a sample procedure using a pendant pipe:

1. Determine a hard surface ceiling location, and use the four mounting holes on the pendant head to mark the positions where holes will be drilled to secure the pendant head. Note that screws are user-supplied and they should be at least 11mm long.

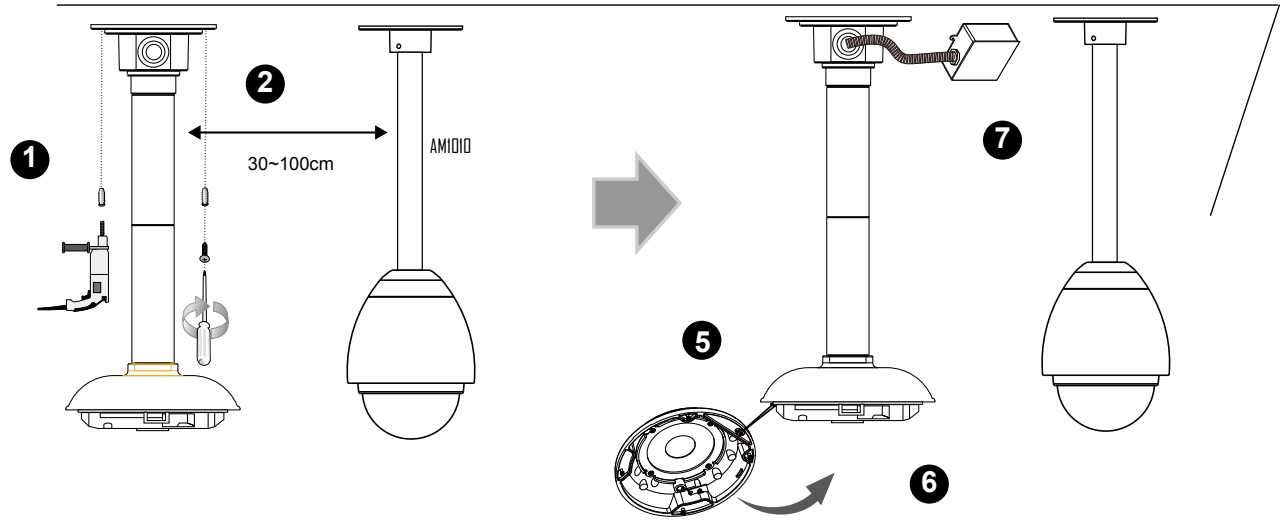


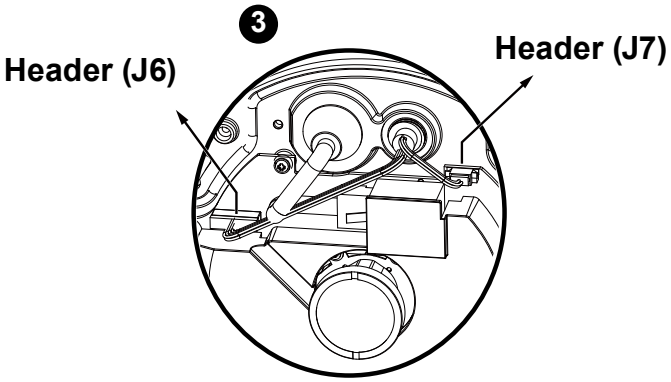

2. Route cables through the pendant pipe and the pendant head.

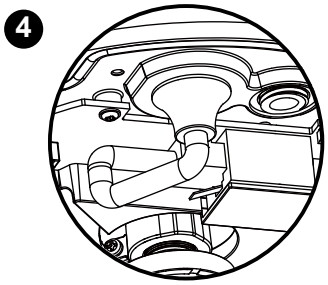


Install to the Ceiling

1. Drill pilot holes into the ceiling. Then hammer four anchors into the holes.
2. Secure the pendant head to the ceiling using four screws.
3. Connect the two white header connectors to the J6 and J7 connectors.
4. Connect the Ethernet cable to the RJ-45 socket.
5. You will find a desiccant bag attached to the camera. Replace the desiccant bag included in the camera with the one shipped within the accessory bag. (SF8172V only)
6. Attach the dome cover to the camera by driving its anti-tamper screws.
7. Route cables through a 3/4” conduit from the pendant head.



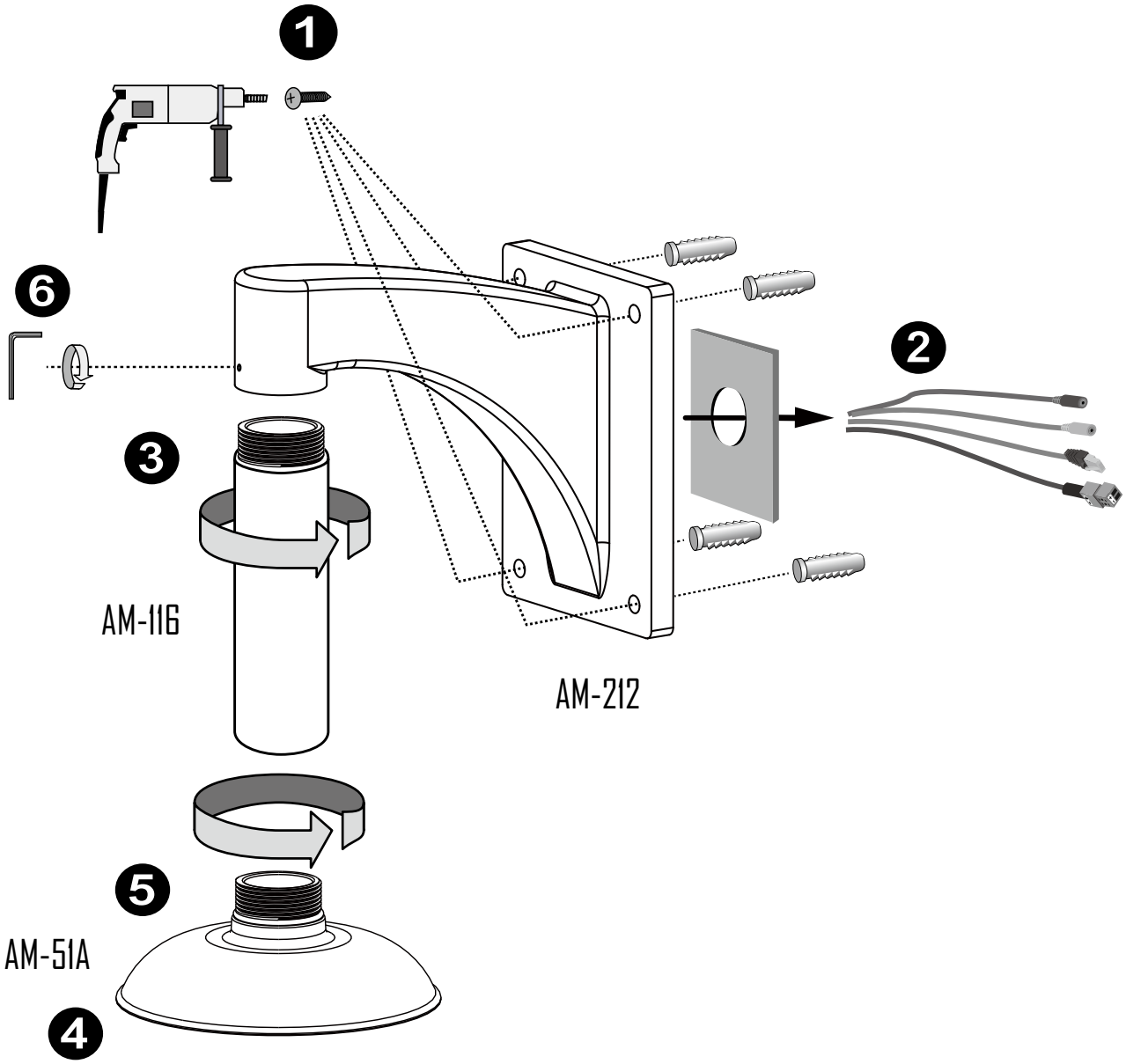

**NOTE:**

Arrange the cables neatly to avoid getting in the way when the dome cover is attached.

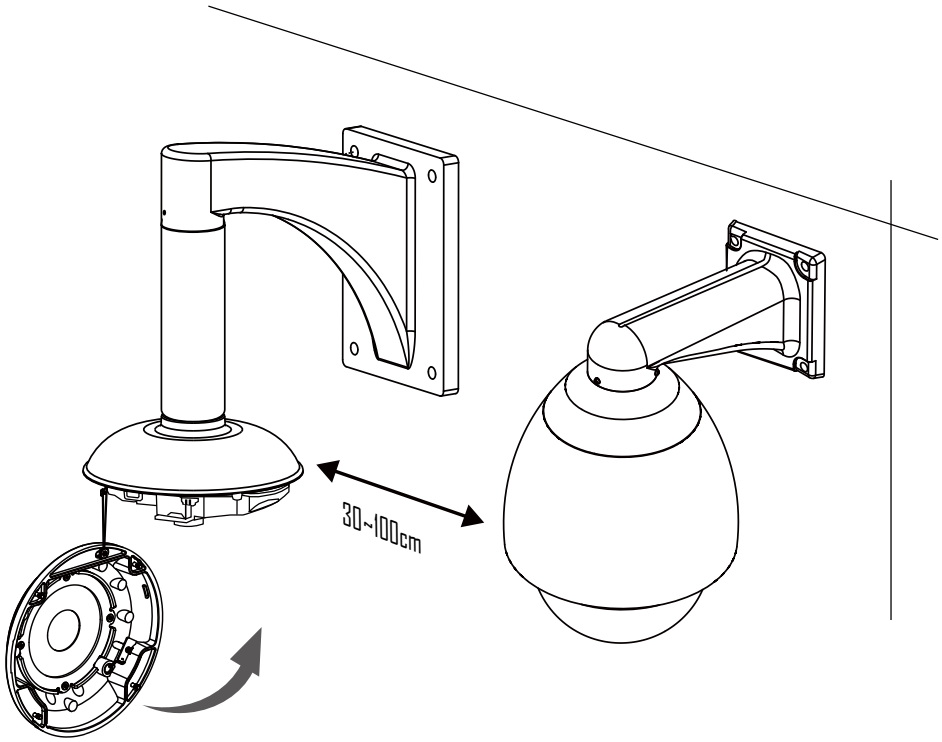
**Wall Mount Bracket Installation**

Below is a sample procedure using a wall mount bracket and a pendant pipe:

1. Determine a hard surface ceiling location. Use the four mounting holes on the wall mount bracket to mark the positions where holes will be drilled to secure the bracket and routing cables. Note that screws are user-supplied and they should be at least 11mm long.
2. Feed cables through the bracket.
3. Install the pendant pipe.
4. Install the camera to the mounting adapter. See Attach Camera to Mounting Adapter on the previous page.
5. Install the mounting adapter to pendant pipe.
6. Tighten the connection using the included hex wrench.



7. Install the speed dome camera next to the fisheye, with their lens positioned at approximately the same height. For details about speed dome installation, please refer to its documentation.
8. Connect all cabling, including the IO cables to J6 and J7, and the Ethernet cable to RJ-45 connector.
9. Install the dome cover by fastening the anti-tamper screws.



# Network Deployment

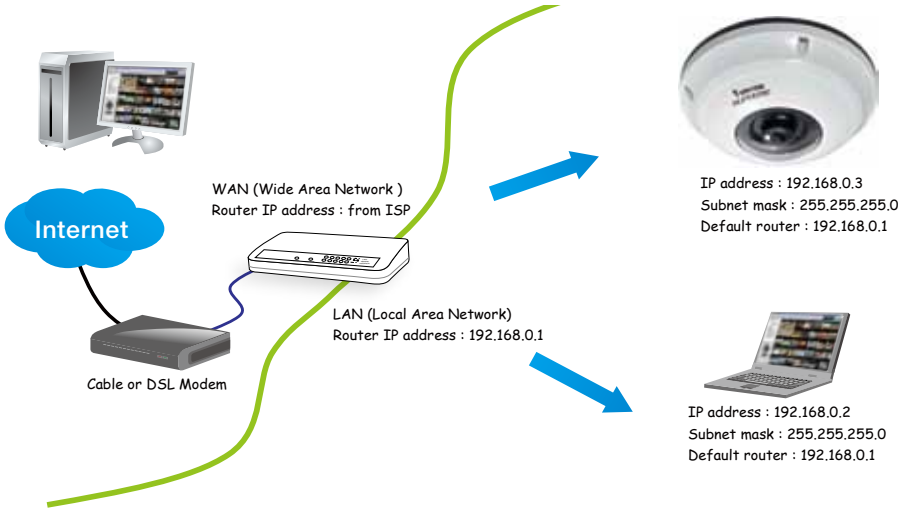
## Setting up the Network Camera over the Internet

There are several ways to set up the Network Camera over the Internet. The first way is to set up the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

### Internet connection via a router

Before enabling the access to the Network Camera over the Internet, make sure you have a router and follow the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated below. Regarding how to obtain your IP address, please refer to Software Installation on page 21 for details.




2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.
   - Secondary HTTP port: 8080
   - RTSP port: 554
   - RTP port for audio: 5558
   - RTCP port for audio: 5559
   - RTP port for video: 5556
   - RTCP port for video: 5557

   If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to your router's user's manual.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 69 for details.

### Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN configuration on page 69 for details.

### Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 90 for details.

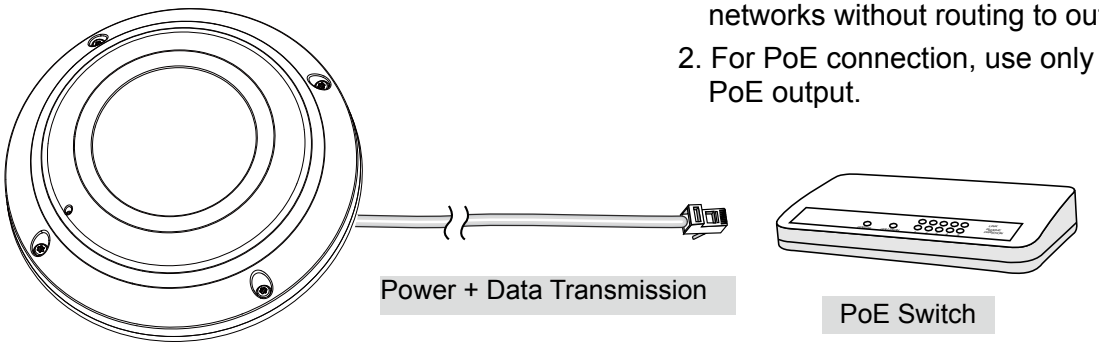
## Set up the Network Camera through Power over Ethernet (PoE)

### When using a PoE-enabled switch

The Network Camera is PoE-compliant, allowing transmission of power and data via a single Ethernet cable. Follow the below illustration to connect the Network Camera to a PoE-enabled switch via an Ethernet cable.

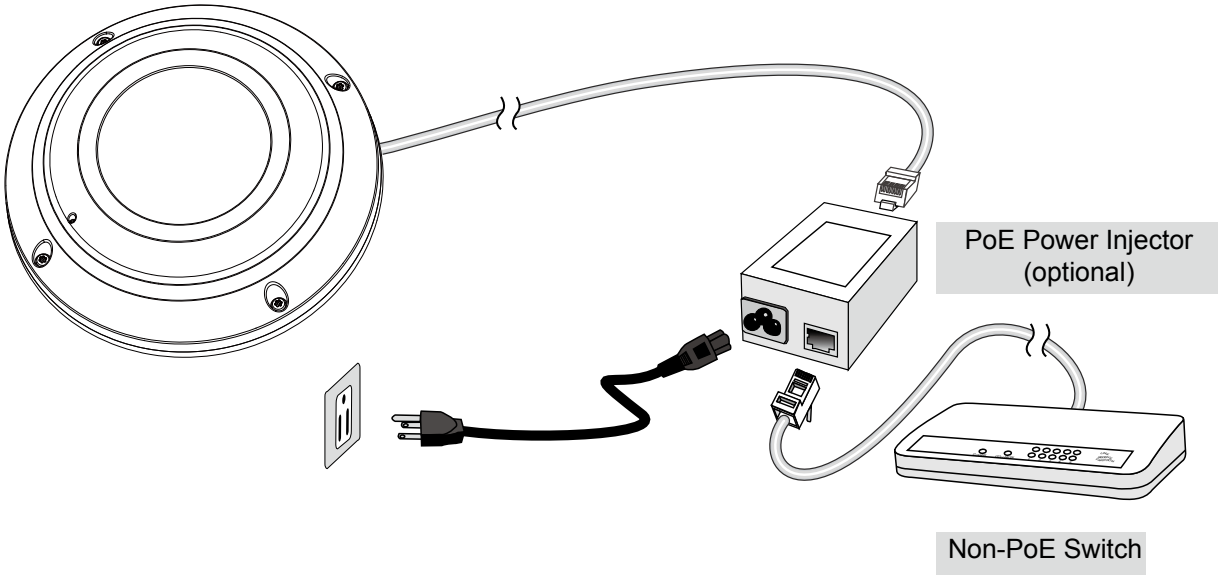
**NOTE:**

1. The camera is only to be connected to PoE networks without routing to outside plants.
2. For PoE connection, use only UL listed I.T.E. with PoE output.



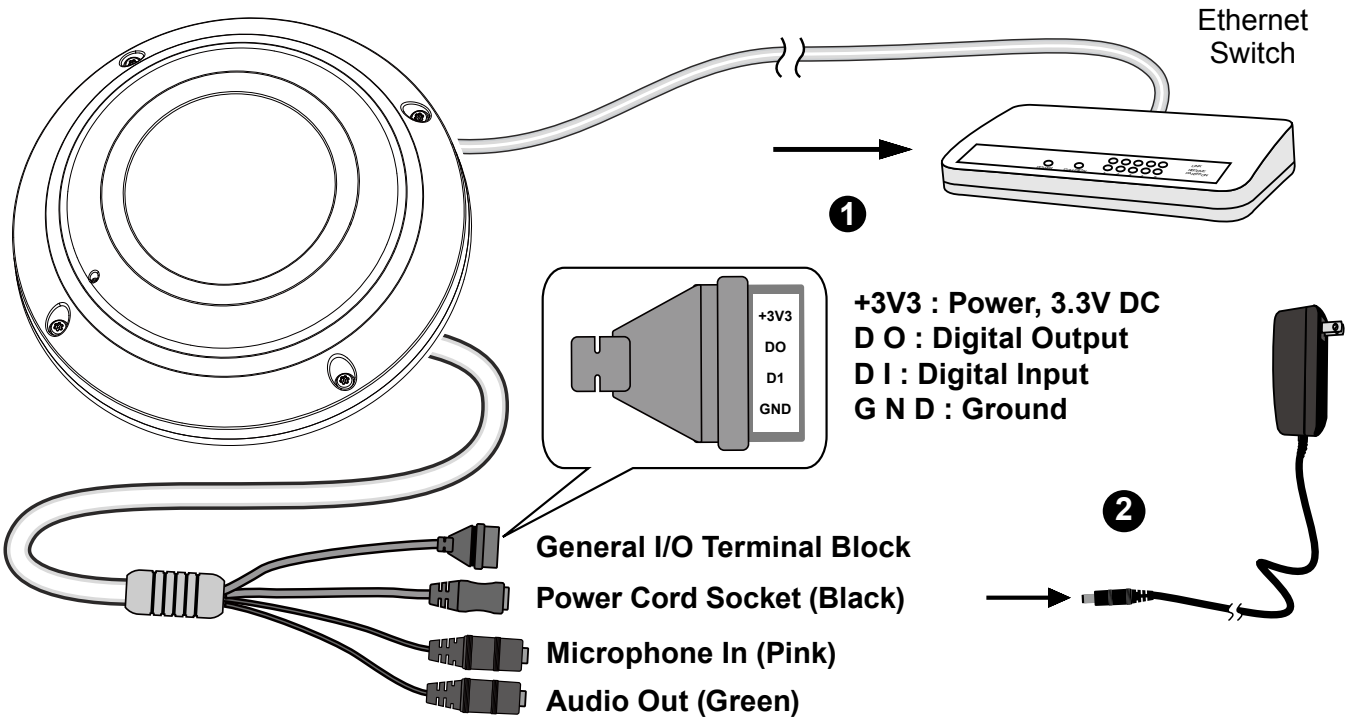

### When using a non-PoE switch

If your switch/router does not support PoE, use a PoE power injector (optional) to connect between the Network Camera and a non-PoE switch.



## General Connection (without PoE)

1. If you have external DI devices, make the connection from general I/O terminal block.
2. Ethernet, power and IO cables are user-supplied.
3. Connect DC power cord to a DC Adapter, and then to a power outlet.




**NOTE:**

The power adapter should comply with L.P.S. regulations featuring O/P: 12V DC, 1.5A min.

# Software Installation

Installation Wizard 2 (IW2), free-bundled software included on the product CD, helps you set up your Network Camera on the LAN.

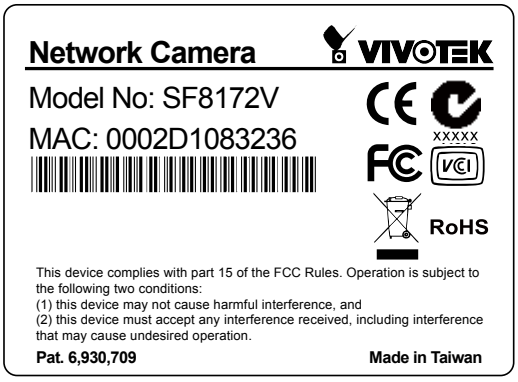
1. Install IW2 under the Software Utility directory from the software CD. Double click the IW2 shortcut on your desktop to launch the program.

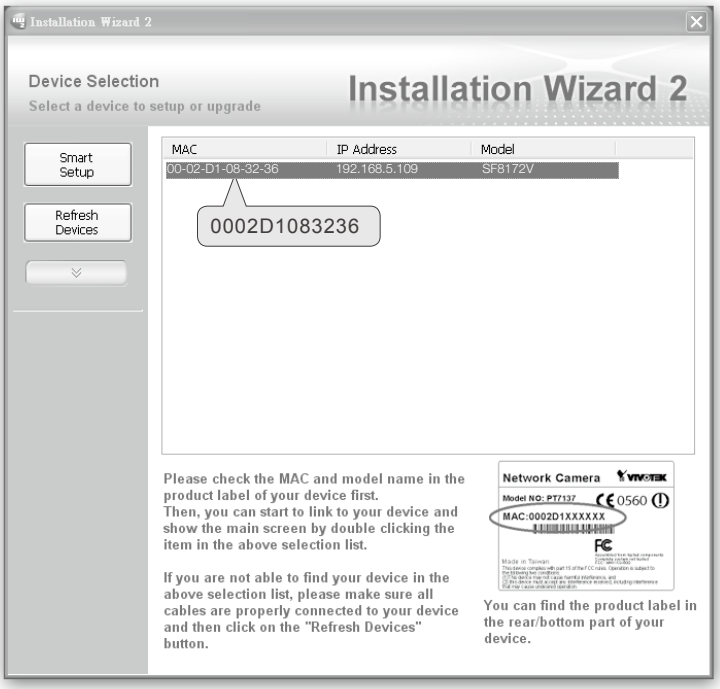

2. The program will conduct an analysis of your network environment. After your network environment is analyzed, please click **Next** to continue the program.



3. The program will search for all VIVOTEK network devices on the same LAN.

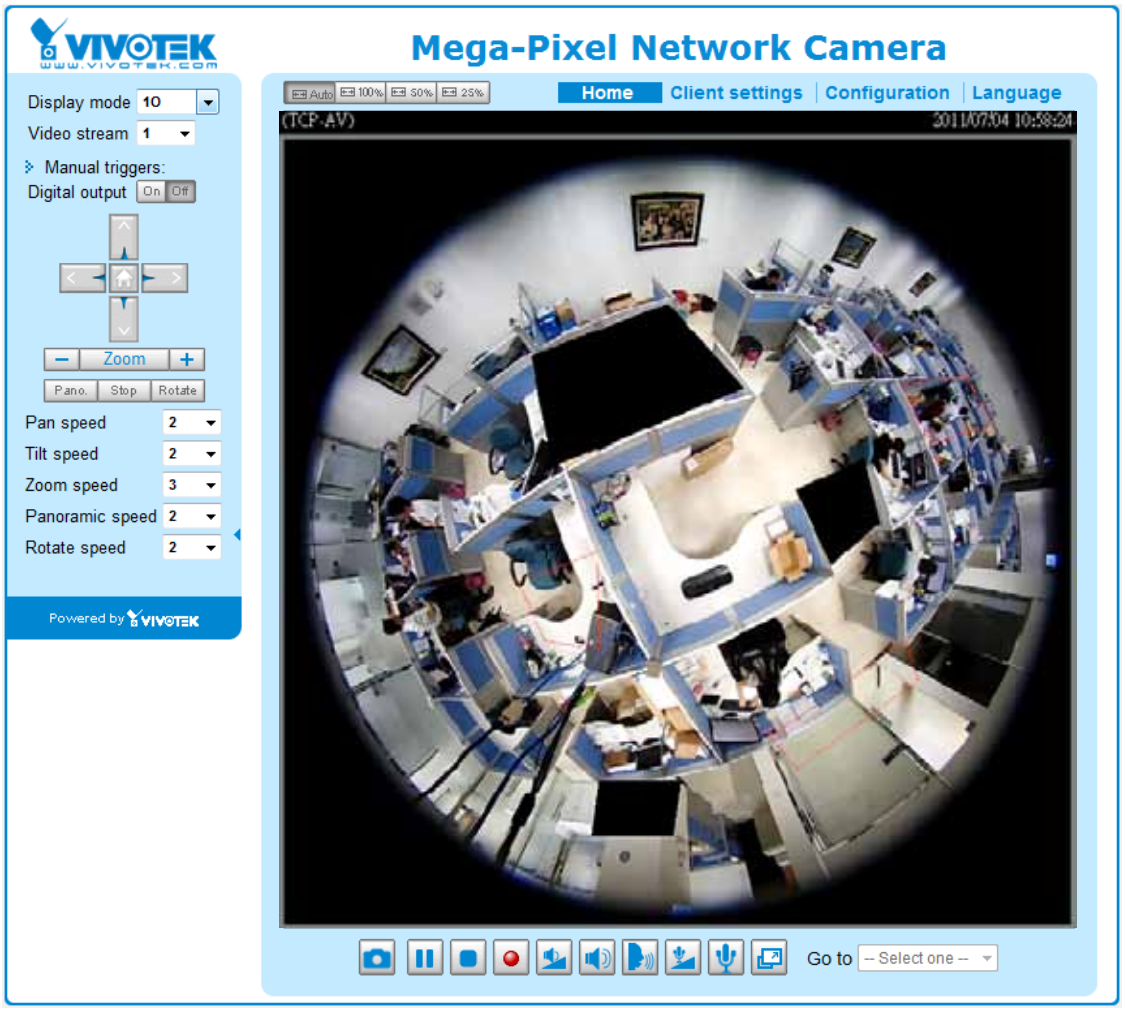
4. After a brief search, the main installer window will pop up. Double-click on the MAC address that matches the one printed on the camera label or the S/N number on the package box label to open a browser management session with the Network Camera.



## Ready to Use

1. A browser session with the Network Camera should prompt as shown below.
2. Refer to the “Panoramic PTZ Installation Guide” in your product CD for the rest of the configuration details.



# Accessing the Network Camera

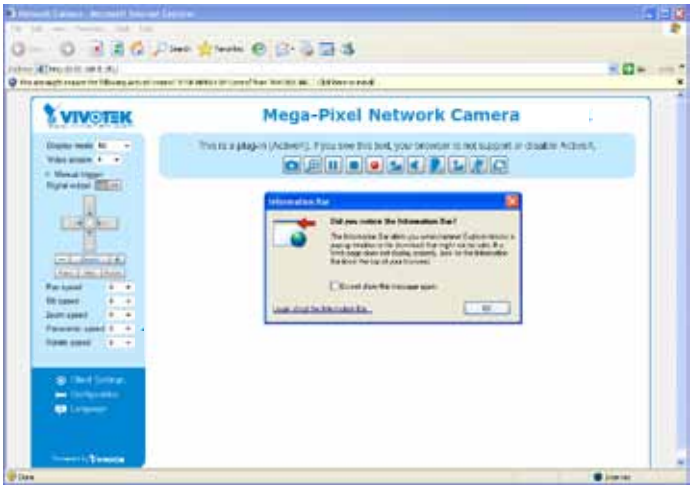
This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

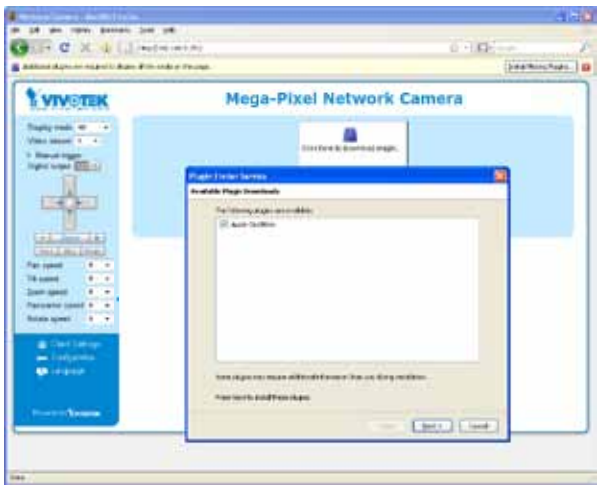
## Using Web Browsers

**IMPORTANT:**

- Currently the Network Camera utilizes 32-bit ActiveX plugin. You **CAN NOT** open a management/view session with the camera using a 64-bit IE browser.
- If you encounter this problem, try execute the Iexplore.exe program from C:\Windows\SysWOW64. A 32-bit version of IE browser will be installed.
- On Windows 7, the 32-bit explorer browser can be accessed from here: C:\Program Files (x86)\Internet Explorer\iexplore.exe

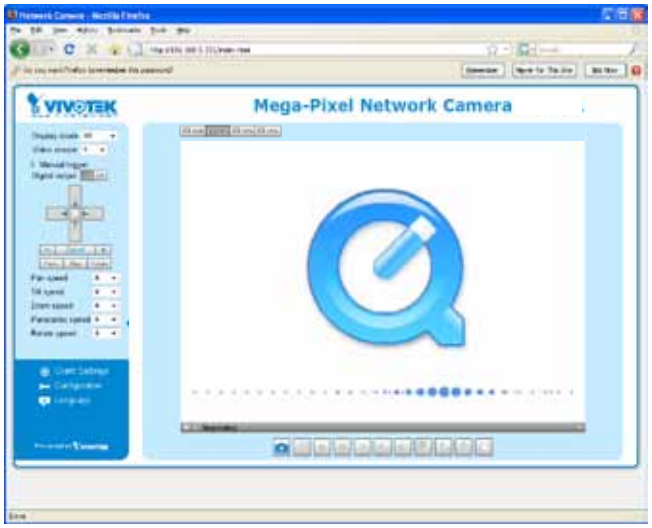
Use Installation Wizard 2 (IW2) to access to the Network Cameras on the LAN.
If your network environment is not a LAN, follow these steps to access the Netwotk Camera:
1. Launch your web browser (e.g., Microsoft® Internet Explorer, Mozilla Firefox, or Netscape).
2. Enter the IP address of the Network Camera in the address field. Press **Enter**.
3. The live video will be displayed in your web browser.
4. If it is the first time installing the VIVOTEK network camera, an information bar will prompt as shown below. Follow the instructions to install the required plug-in on your computer.

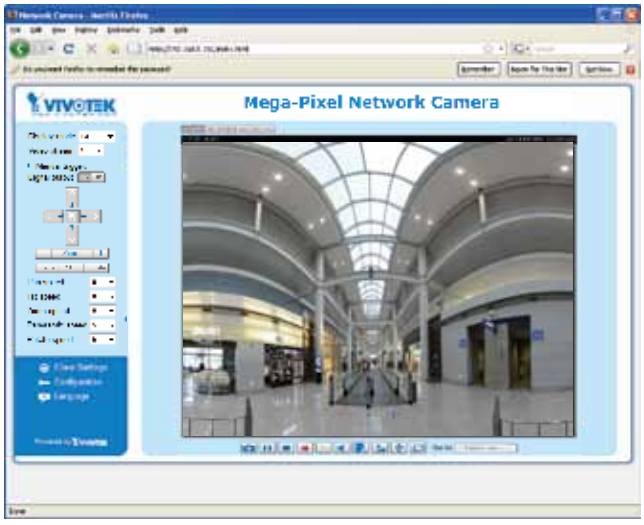


**NOTE:**

For **Mozilla Firefox** or **Netscape** users, your browser will use **Quick Time** to stream live video. If you do not have Quick Time on your computer, please download Quick Time from Apple Inc's website, and then launch your web browser.



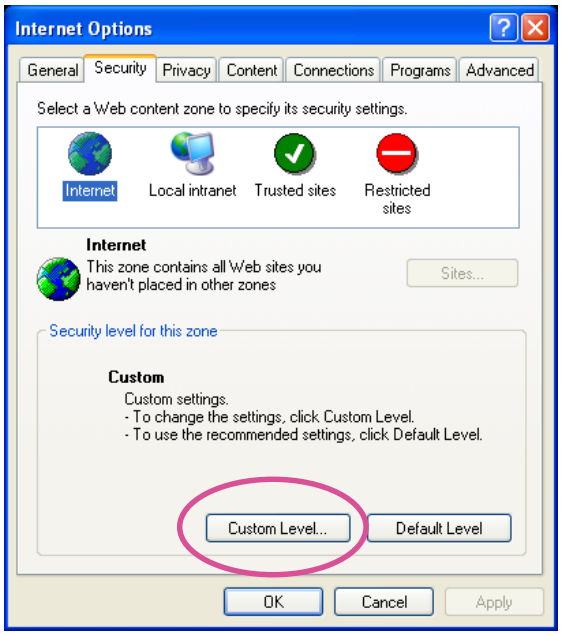



**NOTE:**

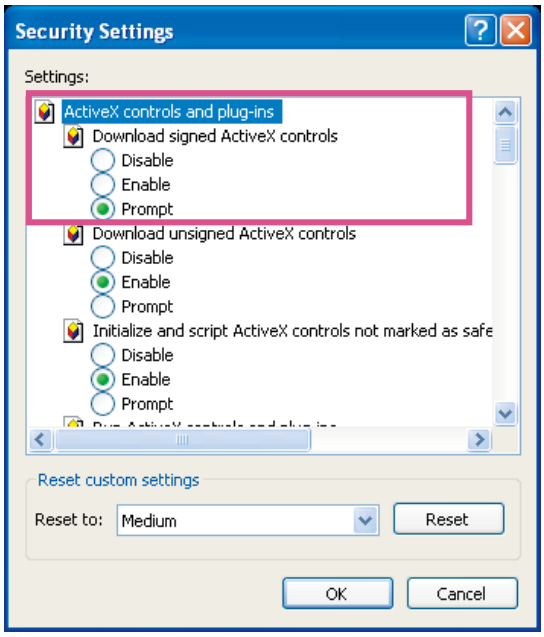
1. By default, your Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to configure a password for your camera later. *For more information about how to enable password protection, please refer to Security on page 88*.
2. If you see a dialogue box indicating that your security settings prohibit running ActiveX Controls®, please enable ActiveX Controls for your browser.

To enable the ActiveX® Controls for your browser:

2-1. Choose Tools > Internet Options > Security > Custom Level.




2-2. Look for Download signed ActiveX® controls; select Enable or Prompt. Click **OK**.




2-3. Refresh your web browser, then install the ActiveX® control. Follow the instructions to complete installation.

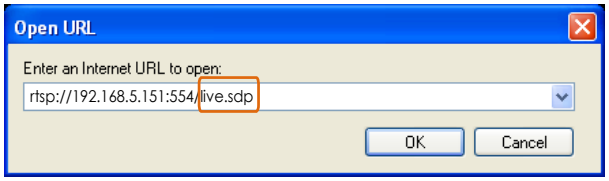
## Using RTSP Players

To view the H.264/MPEG-4 streaming media using RTSP players, you can use one of the following players that support RTSP streaming.

Quick Time Player
Real Player

1. Launch the RTSP player.
2. Choose File > Open URL. A URL dialog box will prompt.
3. The address format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 to stream4>

As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 78.
For example:




4. The live video will be displayed in your player. For more information on how to configure the RTSP access name, please refer to RTSP Streaming on page 78 for details.


The RTSP players will show the original circular image. You can access the Regional views via the ST7501 or VAST software. See page 79 for an example.

## Using 3GPP-compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 18.

To utilize this feature, please check the following settings on your Network Camera:

1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable.
   For more information, please refer to RTSP Streaming on page 78.

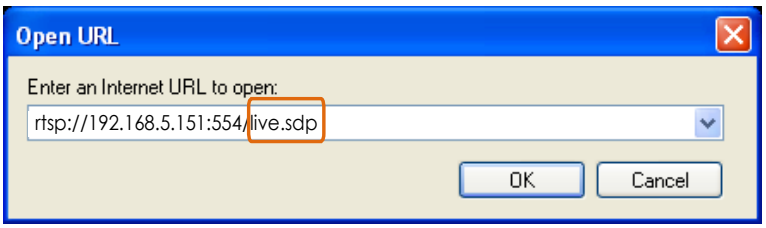
2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video and audio streaming parameters as listed below.
   For more information, please refer to Stream settings on page 64.

| | |
|---|---|
| Video Mode | MPEG-4 |
| Frame size | 176 x 144 |
| Maximum frame rate | 5 fps |
| Intra frame period | 1S |
| Video quality (Constant bit rate) | 40kbps |
| Audio type (GSM-AMR) | 12.2kbps |

3. As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 78.

4. Launch the player on the 3GPP-compatible mobile devices (e.g., Real Player).

5. Type the following URL commands in the URL field.
   The address format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream 3>.
   For example:



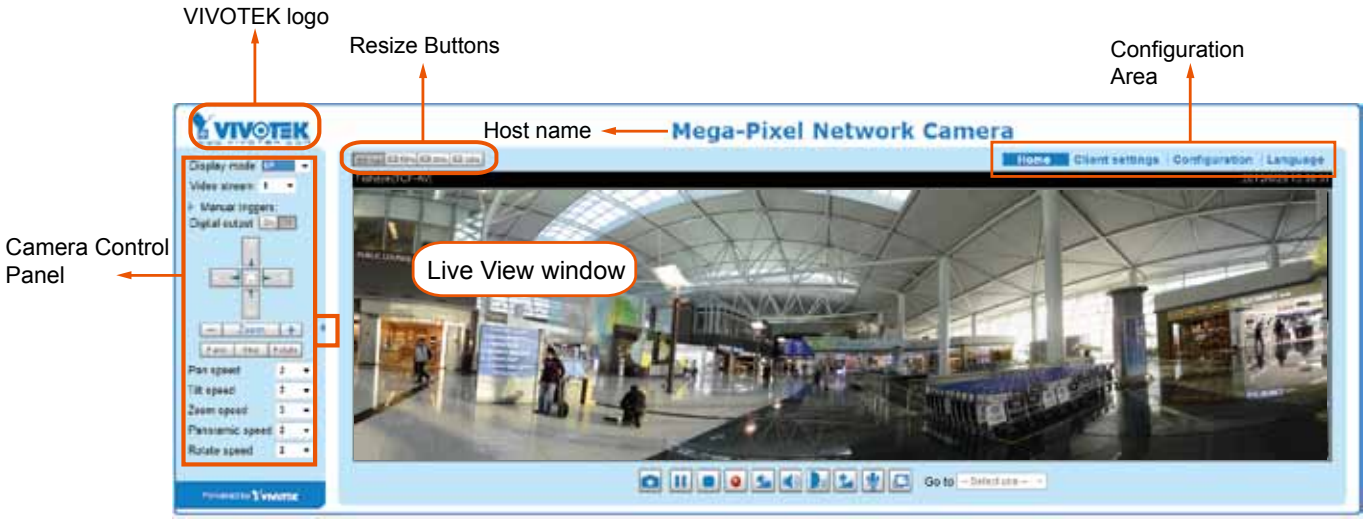
## Using VIVOTEK Recording Software

When this camera is installed in a Panoramic PTZ configuration, the Panoramic PTZ functionality is managed either through VIVOTEK's VAST software or Milestone's XProtect. Please refer to the "Panoramic PTZ Installation Guide" in your product CD for configuration details.

Please install the recording software; then launch the program to add the Network Camera to the Channel list. For detailed information about how to use the recording software, please refer to the user's manual of the software or download it from http://www.vivotek.com.

# Main Page

This chapter explains the screen elements on the main page. It is composed of the following sections: VIVOTEK INC. Logo, Host Name, Camera Control Area, Configuration Area, and Live Video Window.




## VIVOTEK INC. Logo

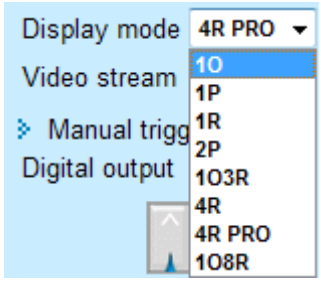
Click this logo to visit the VIVOTEK website.

## Host Name

The host name can be customized to fit your needs. For more information, please refer to System > General Settings on page 42.

## Camera Control Area

**Display mode:** This is a brand new configuration menu exclusively designed for Fisheye cameras. Due to the fisheye lens' wide coverage of 180º hemispheric and 360º panoramic views and to manipulate the details within, the following display modes are provided:




**1O** - One Original fisheye view.
**1P** - One Panoramic view
**1R** - One Regional view
**2P** - Two Panoramic views
**1O3R** - One Original and three Regional views
**4R** - Four Regional views
**4R PRO** - Four Regional views interactively displayed when the field of view changes in any of the views
**1O8R** - One Original and eight Regional views

* See following discussions for detailed explanation of these modes. The Wall mount type provides another two distinctive modes.

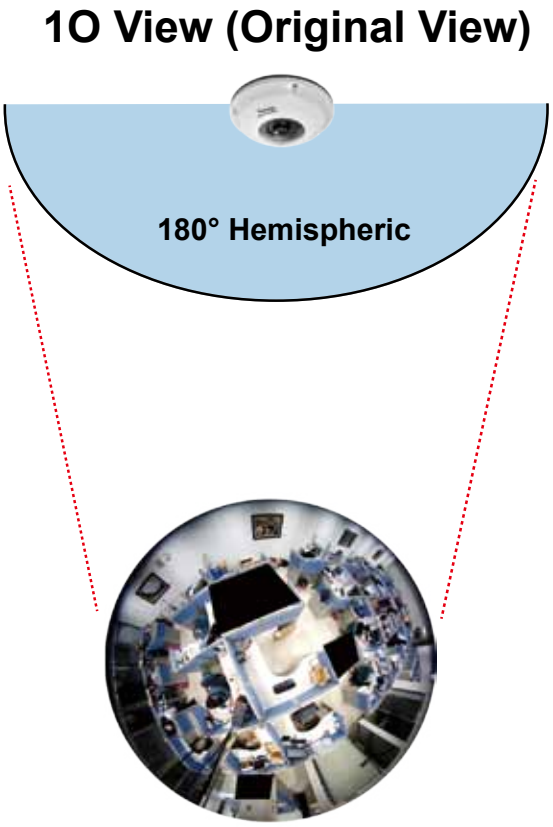
**NOTE:**

The following fisheye modes will not be available if you select the "1080P Full HD" mode in the Media > Video configuration window. The 1080P Full HD mode is like using the fisheye as an ordinary HD camera.


### 1O (Original) Display mode:

When mounted on a ceiling, the fisheye camera can cover an approximately 50 m² of surveillance area (hung at a height of approximately 3 meters), while still keeping details in videos with recognizable facial features of people trafficking through the area.

The 1O view is especially adequate for taking an over-view glimpse of surveillance area with a ceiling mount camera.



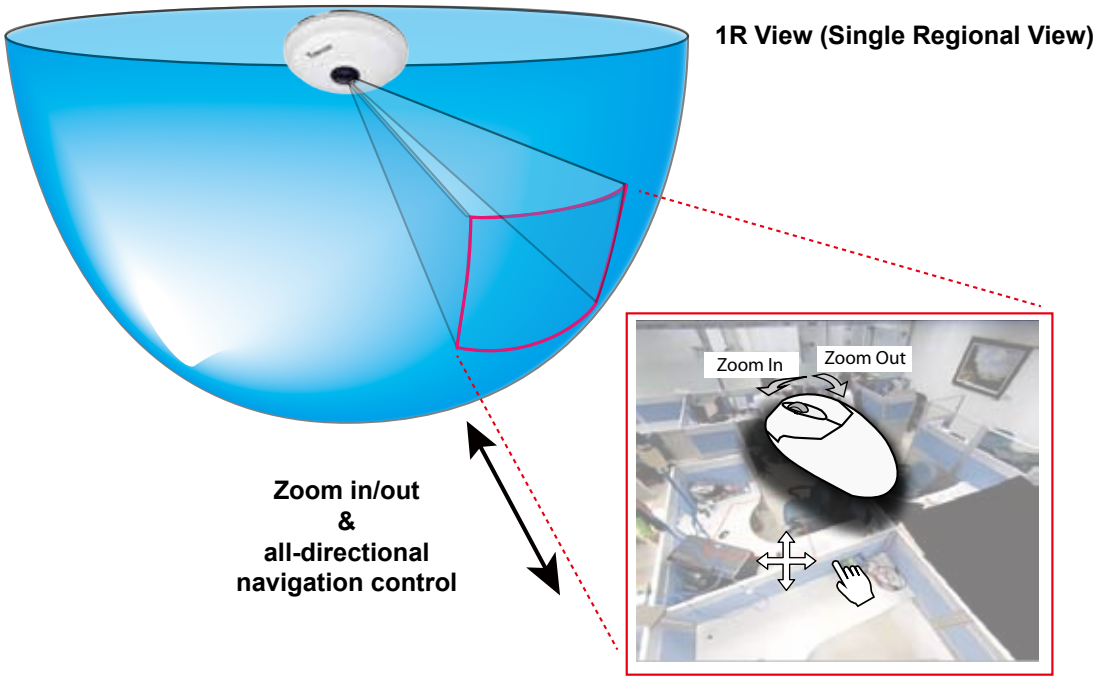

### 1P (Single Panoramic) Display mode:

With image correction firmware algorithms, the hemispheric image is transformed into a rectilinear stripe in the 1P display mode. Viewers can use the PTZ panel or simply use mouse control to quickly move through the 360º panoramic view.

Note that the 1P view is apt for an overview, the Zoom in/out function does not apply in this mode.

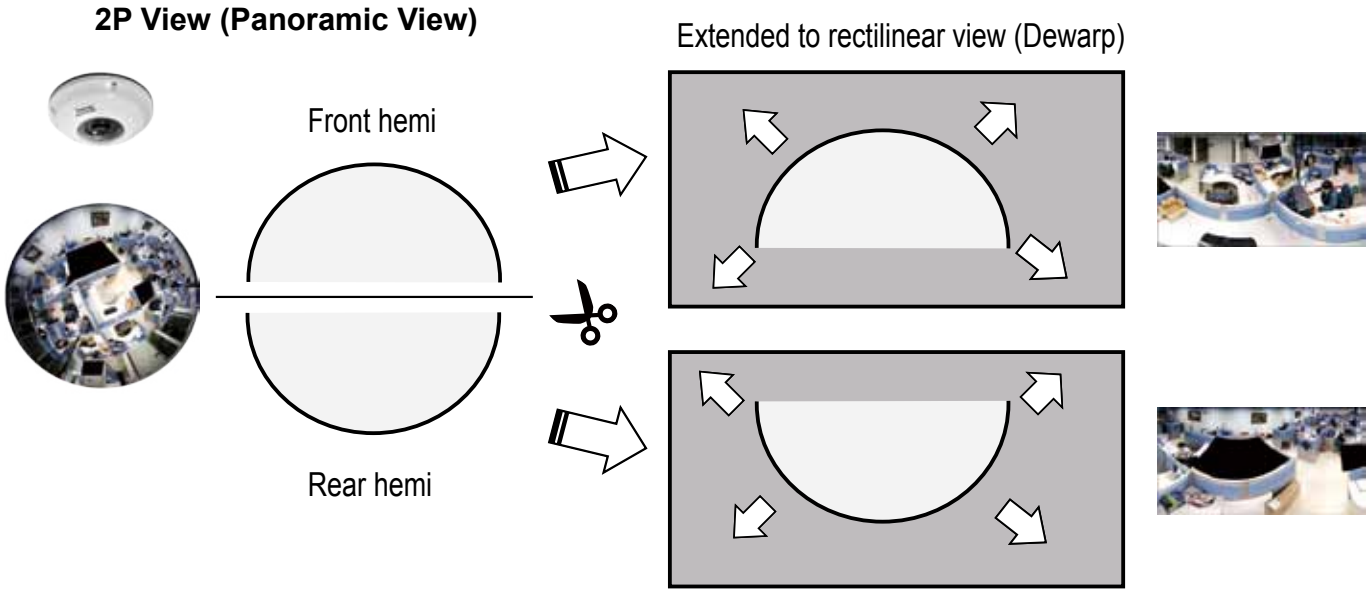
## 1R (Single Regional) Display mode:

The 1R mode provides access to one image section within the hemisphere. You can zoom in or out (using the mouse wheel or PTZ panel) or travel through to other areas within the hemisphere using simple mouse clicks and drags. A single click on a particular object can bring the object to the center of your view window. Click and hold down the left mouse button, and you can swipe the view both horizontally and vertically.




## 2P (Dual Panoramic View) Display mode:

Similar to 1P, the 2P display mode provides simultaneous access to both the front and rear sections of a hemisphere. Both panoramic views are corrected into a more viewable dewarped image. Viewers can use a mouse click and drag to quickly scroll horizontally through the surveillance area.



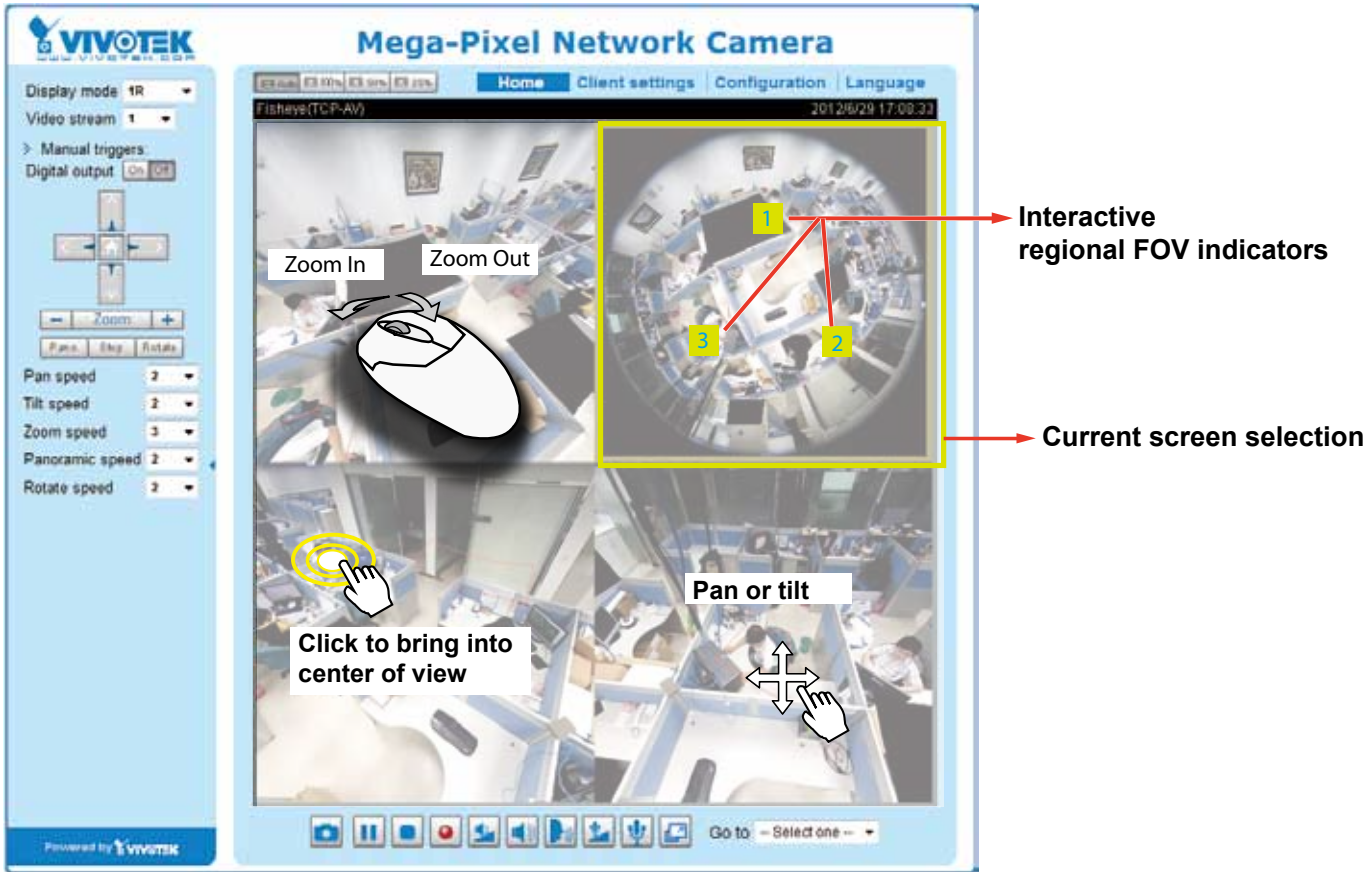
## 1O3R (One Original & Three Regional) Display mode:

The 1O3R mode provides access to multiple live view sections within the hemisphere and the reference to their relative positions on an Original circular view. The FOV indicators (#1 ~ #3) interact with your current operation as you may zoom in/out or move the live view sections elsewhere.

You can zoom in or out or travel to other areas within the hemisphere using identical methods as previously described in the 1R mode.

You can also change the locations of Regional views by dragging the FOV indicators on the "Original" round-shape circular view.

### 1O3R (Original & Regional) Mode Screen Control




**Tips:**

In a Regional view displaying 100% of video feed (via the Resize buttons - see page 35), your mouse wheel can be used to scroll the view window vertically before you click on a live image. After you click on the live image, the mouse wheel becomes the zoom in/out tool.

### 4R (Four Regional) Display mode:

The view control and look and feel are identical to that as described in the 1O3R mode except the absence of the Original circular view.

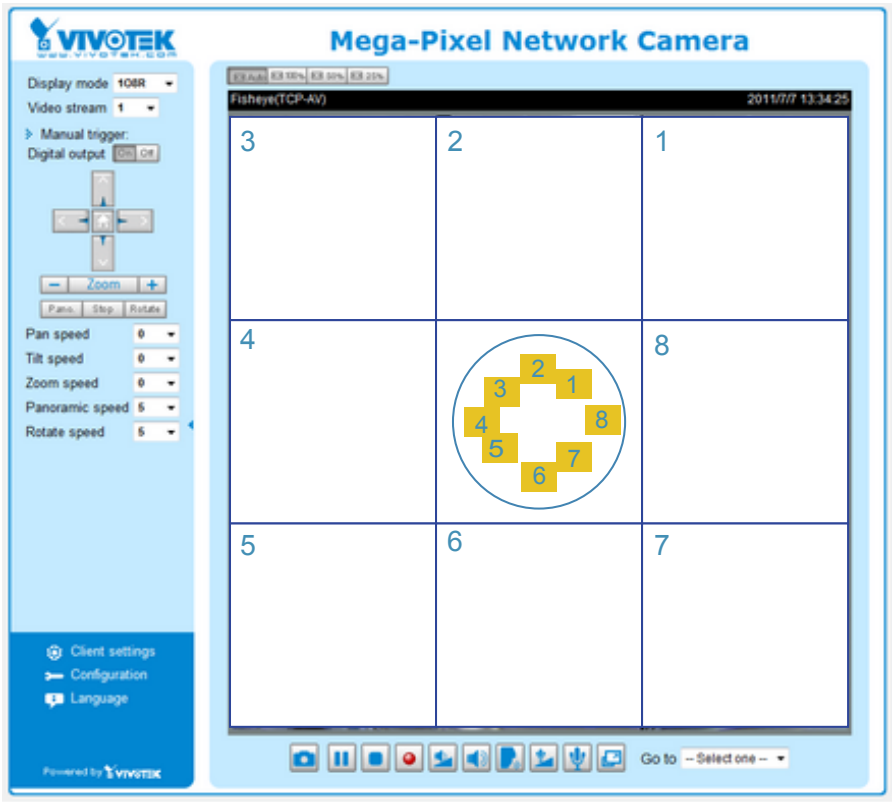
### 4R PRO (Four Regional Proactive) Display mode:

The 4R PRO mode is similar to the 4R mode except that the quad view windows consecutively rotate in correspondence to the change of view area in one window. Note that zoom in/out and tilt control is not available in this mode.

### 1O8R (One Original and Eight Regional) Display mode:

The view control and look and feel are identical to that as described in the 1O3R mode.

Note that if you change the position of a view in hemisphere, e.g., #3 window, you may lose the configuration change by switching to another display mode. The live view window does not automatically save your view section layout.




### 1P2R (One Panoramic and Two Regional) Display mode:
### 1P3R (One Panoramic and Three Regional) Display mode:

These two modes are only available with the **Wall Mount type**! The Mount type configuration is found in **Configuration > Media > Image > General Settings**. Please refer to page 53 for details.

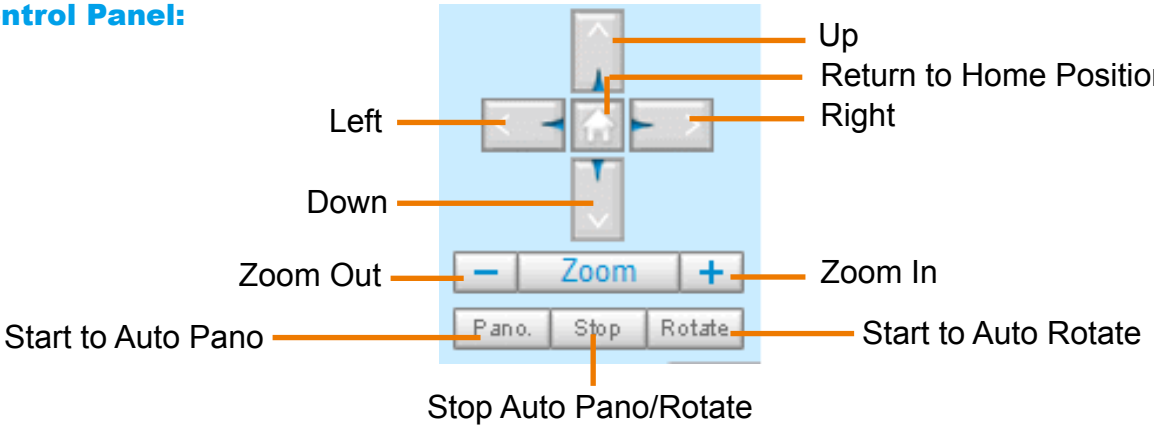
The view control in these two modes is identical to that as described in the 1O3R mode.

Video Stream: This Network Cmera supports multiple streams (stream #1 ~ #3) simultaneously. You can select any one of them for live viewing. For more information about multiple streams, please refer to page 63 for detailed information.

Manual Trigger: Click to enable/disable an event trigger manually. Please configure an event setting before enabling this function. A total of 3 or 4 event settings can be configured. For more information about event setting, please refer to page 104. If you want to hide this item on the homepage, please go to the **System > Homepage Layout > General settings > Customized button** to deselect the "show manual trigger button" checkbox.

Digital Output: Click to turn the digital output device on or off.

**PTZ Control Panel:**




Pano.: Click this button to start the automated circular rotation through a regional view (360° continuous rotation). Note that this function does not apply in a Panoramic view because a Panoramic view already shows the full coverage.

Stop: Click this button to stop the Auto Pano and Auto Rotate functions.

Rotate: Once the Administrator has determined a list of preset **PTZ** positions, click this button to command the camera to consecutively display views of these positions. The Network Camera will display these views continuously. For more information, **please refer to PTZ settings on page 101.**

| Pan speed | Tilt speed | Zoom speed | Panoramic speed | Rotate speed | |
|---|---|---|---|---|---|
| -5 | -5 | -5 | - | - | Slower |
| -4 | -4 | -4 | - | - | |
| -3 | -3 | -3 | - | - | |
| -2 | -2 | -2 | - | - | |
| -1 | -1 | -1 | - | - | |
| 0 | 0 | 0 | 0 | 0 | |
| 1 | 1 | 1 | 1 | 1 | |
| 2 | 2 | 2 | 2 | 2 | |
| 3 | 3 | 3 | 3 | 3 | |
| 4 | 4 | 4 | 4 | 4 | |
| 5 | 5 | 5 | 5 | 5 | Faster |

Pan /Tilt /Zoom /Panoramic/Rotate: Adjust the speed of these controls:

## Configuration Area

Client Settings: Click this button to access the client setting page. For more information, please refer to Client Settings on page 39.

Configuration: Click this button to access more of the configuration options provided with the Network Camera. It is suggested that a password is applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to the description for the Configuration menus on page 41.

Language: Click this button to choose a language for the user interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文. You can also change a language on the Configuration page; please refer to page 41.

## Hide Button

You can click the hide button to hide the control panel or display the control panel.

## Resize Buttons

:

Click the Auto button, the video cell will resize automatically to fit the monitor.
Click 100% is to display the original homepage size.
Click 50% is to resize the homepage to 50% of its original size.
Click 25% is to resize the homepage to 25% of its original size.

## Live Video Window

■ The following window is displayed when the video mode is set to H.264 / MPEG-4:


Video Title: The video title can be configured. For more information, please refer to Video settings on page 64.

H.264 / MPEG-4 Protocol and Media Options: The transmission protocol (TCP or UDP, etc.)and media options for H.264 / MPEG-4 video streaming. For further configuration, please refer to Client Settings on page 39.

Time: Display the current time. For further configuration, please refer to Media > Image > Genral settings on page 53.

Title and Time: The video title and time can be stamped on the streaming video. For further configuration, please refer to Media > Image > Genral settings on page 53.

Video and Audio Control Buttons: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Pause: Pause the transmission of the streaming media. The button becomes the Resume button after clicking the Pause button.

Stop: Stop the transmission of the streaming media. Click the Resume button to continue transmission.

Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 40 for details.

Volume: When the Mute function is not activated, move the slider bar to adjust the volume on the local computer.

Mute: Turn off the volume on the local computer. The button becomes the Audio On button after clicking the Mute button.

Talk: Click this button to talk to people around the Network Camera. Audio will project from the external speaker connected to the Network Camera. Click this button again to end talking transmission.

Mic Volume: When the Mute function is not activated, move the slider bar to adjust the microphone volume on the local computer. Note that inernal microphone is mounted on the dome cover.

Mute: Turn off the Mic volume on the local computer. The button becomes the Mic On button after clicking the Mute button.

Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

■ The following window is displayed when the video mode is set to MJPEG:


Video Title: The video title can be configured. For more information, please refer to Media > Image on page 53.

Time: Display the current time. For more information, please refer to Media > Image on page 53.

Title and Time: Video title and time can be stamped on the streaming video. For more information, please refer to Media > Image on page 53.

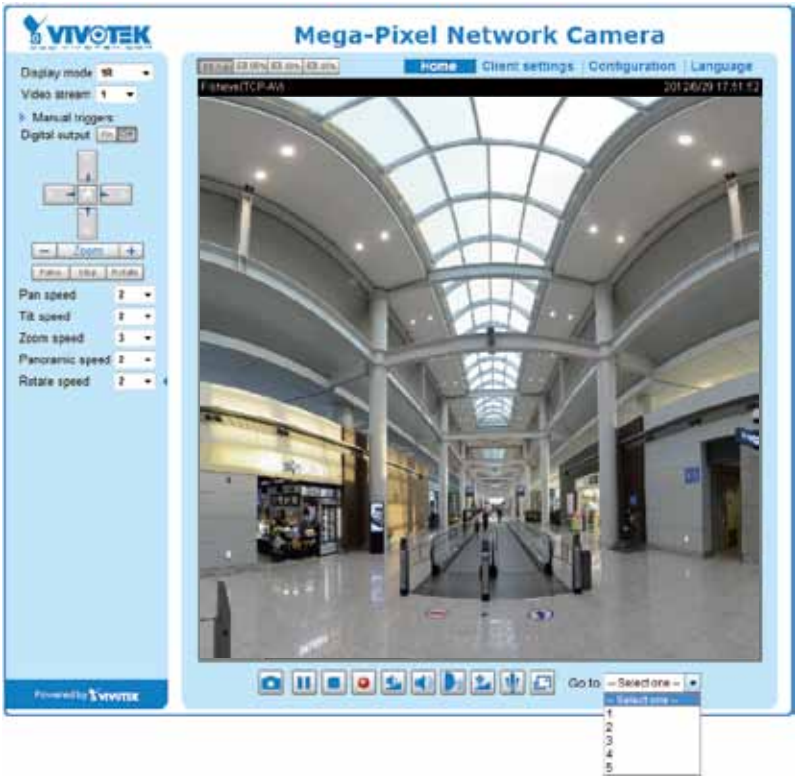
Video Control Buttons: Depending on the camera model and your current configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 40 for details.

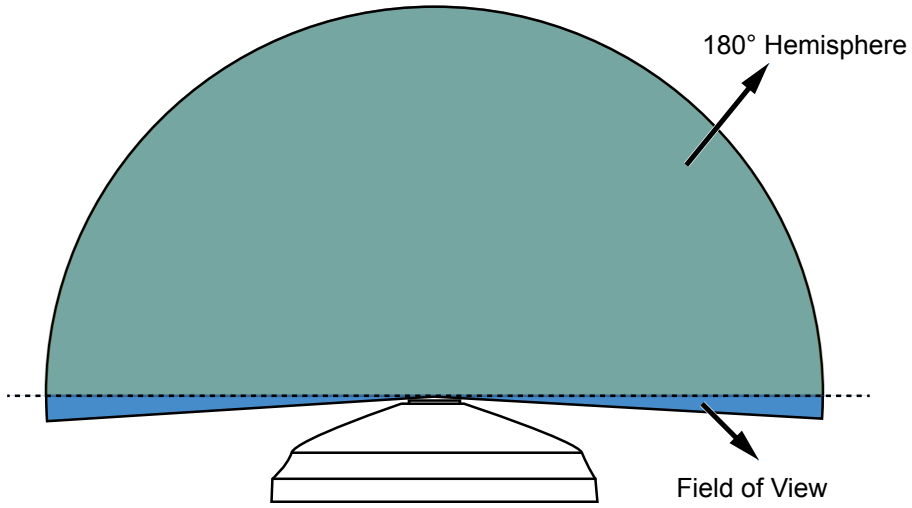
Full Screen: Click this button to switch to full screen mode. Press the “Esc” key to switch back to normal mode.

Go to: Select one preset position from the Go to drop-down list, and the Network Camera’s field of view will move to the position. The PTZ preset positions are also related to the **Rotate** button: Click the button, then the Network Camera's field of view will patrol continuously through the selected positions. Note that the move to a preset position only takes place on the "**R" (Regional Display mode)** window.




Please refer to page 101 for PTZ preset position settings.

**NOTE:**

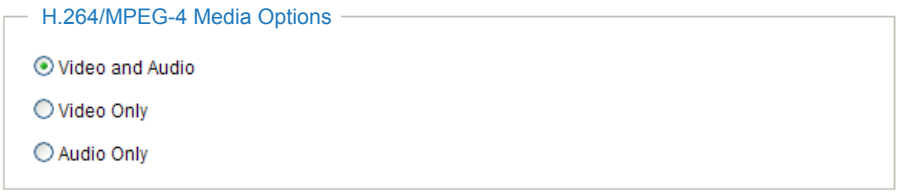



1. Edges of a fisheye circular view will be slightly cropped because the fisheye lens FOV is larger than the sensor can take.
2. The camera lens' angle of view is larger than 180°. Therefore, the camera's circular view is actually larger than a 180° hemisphere.
3. Since the field of view is larger than a hemisphere, for the SF8172V, the top edge of dome cover (the round opening where the lens is installed) will appear as a white circle around an circular view.
4. When using the dewarped modes, e.g., the Regional and Panoramic views, the firmware will not capture the far edges of the FOV which extends beyond the 180° hemisphere.

# Client Settings

This chapter explains how to select the stream transmission mode and saving options on the local computer. When completed with the settings on this page, click **Save** on the page bottom to enable the settings.

## H.264 / MPEG-4 Media Options




Select to stream video or audio data or both. This is enabled only when the video mode is set to H.264 or MPEG-4.

## H.264 / MPEG-4 Protocol Options


Depending on your network environment, there are four options with the transmission protocols with H.264 or MPEG-4 streaming:

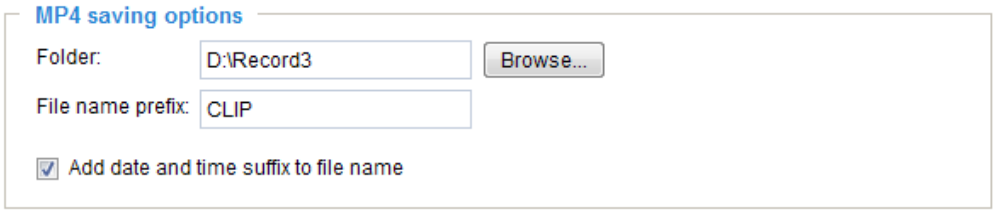
UDP unicast: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up to ten simultaneous accesses.

UDP multicast: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 78.

TCP: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. The downside of this protocol is that its real-time effect is not as good as that of using the UDP protocol.

HTTP: This protocol allows the same quality as TCP protocol without needing to open specific ports for streaming under some network environments. Users behind a firewall can utilize this protocol to allow camera's streaming data to pass through.

## MP4 Saving Options

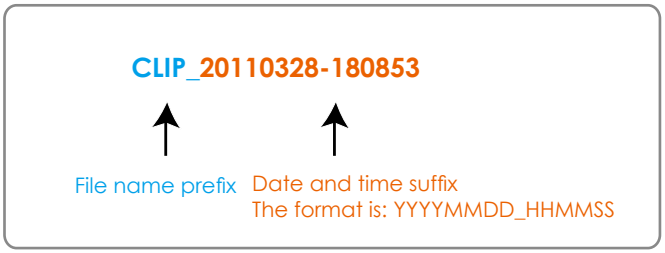



Users can record live video as they are watching it by clicking the  "Start MP4 Recording" button on the main page. Here, you can specify the storage destination and file name.

Folder: Specify a storage destination for the recorded video files.

File name prefix: Enter the text that will be appended to the front of the video file name.

Add date and time suffix to the file name: Select this option to append the date and time to the end of the file name.




## Local Streaming Buffer Time


In a busy network, fluctuations in available bandwidth can occur. Video streaming may lag and may not proceed very smoothly. If you enable this option, video streams from the camera will be temporarily stored on the computer's cache memory for a configurable period of time (seconds or milliseconds) before being played on a web session. This will help you see the streaming more smoothly. If you enter 3000 Millisecond, the streaming will delay for 3 seconds.

# Configuration

Click **Configuration** on the main page to enter the camera setting pages. Note that only Administrators can access the configuration page.

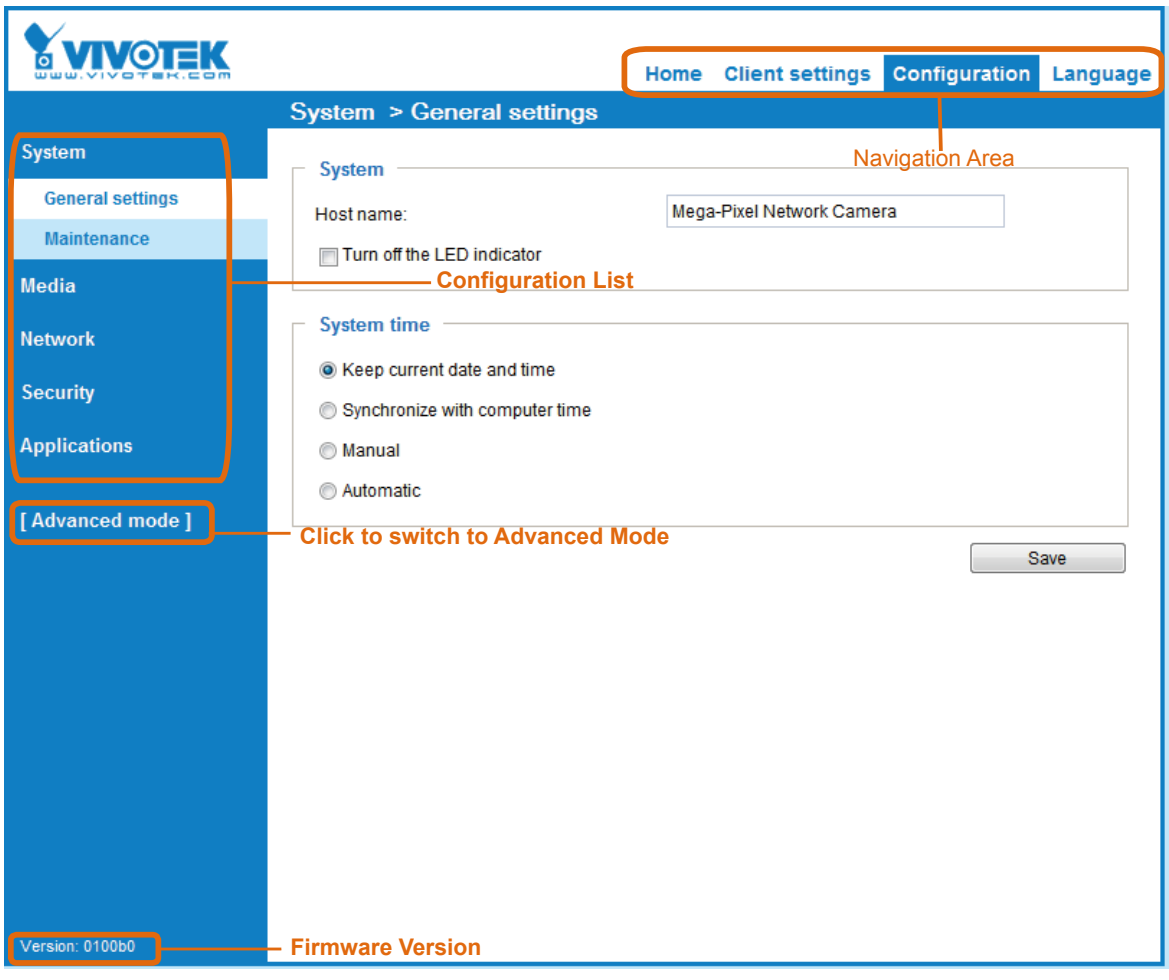
VIVOTEK provides an easy-to-use user interface that helps you set up your network camera with minimal effort. To simplify the setting procedure, two types of user interfaces are available: Advanced Mode for professional users and Basic Mode for entry-level users. Some advanced functions (PTZ/ Event/ Recording/ Local storage) are not displayed in Basic Mode.

If you want to set up advanced functions, please click on **[Advanced Mode]** at the bottom of the configuration list to switch to Advanced Mode.

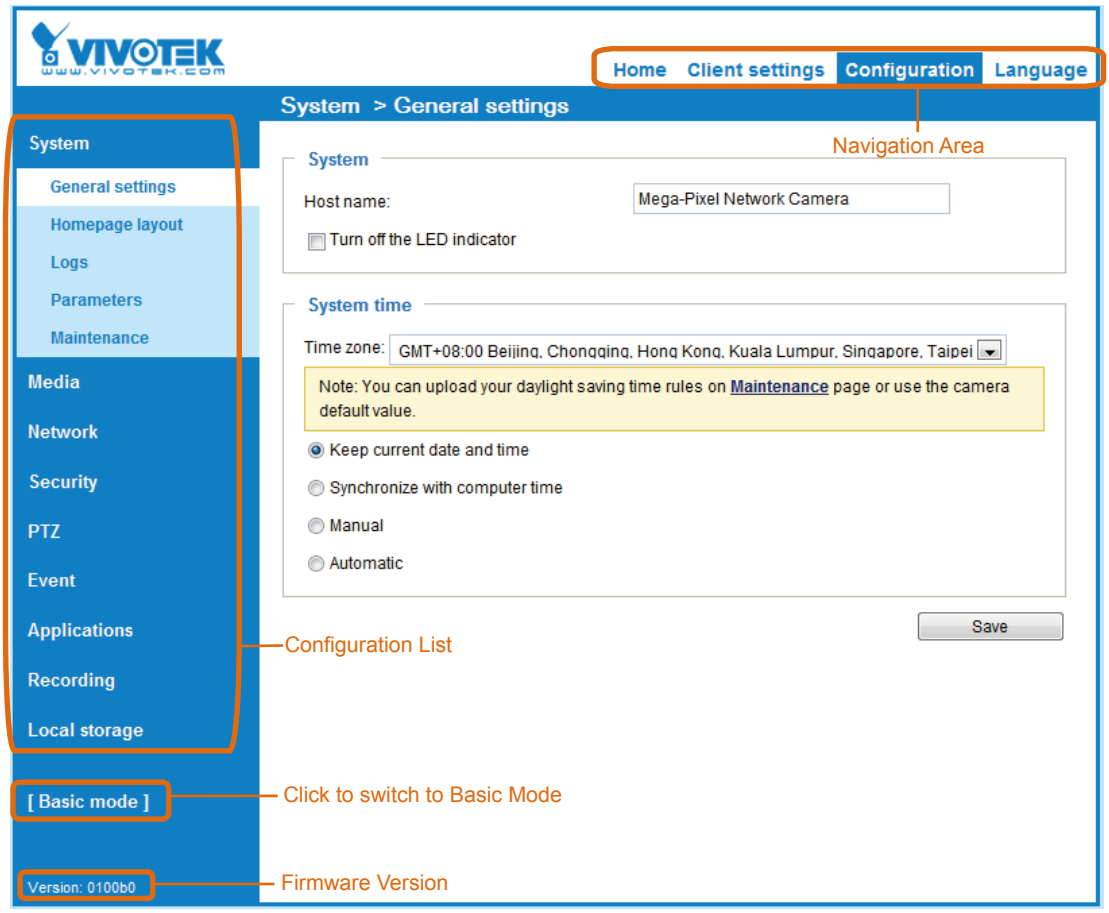
In order to simplify the user interface, detailed information will be hidden unless you click on the function item. When you click on the first sub-item, the detailed information for the first sub-item will be displayed; when you click on the second sub-item, the detailed information for the second sub-item will be displayed and that of the first sub-item will be hidden.

The following is the interface of the Basic Mode and the Advanced Mode:

**Basic Mode**



## Advanced Mode




Each function on the configuration list will be explained in the following sections. Those functions that are displayed only in Advanced Mode are marked with Advanced Mode. If you want to set up advanced functions, please click on **[Advanced Mode]** at the bottom of the configuration list.

The Navigation Area provides access to all different views from the **Home** page (for live viewing), **Configuration** page, and multi-language selection.

# System > General settings

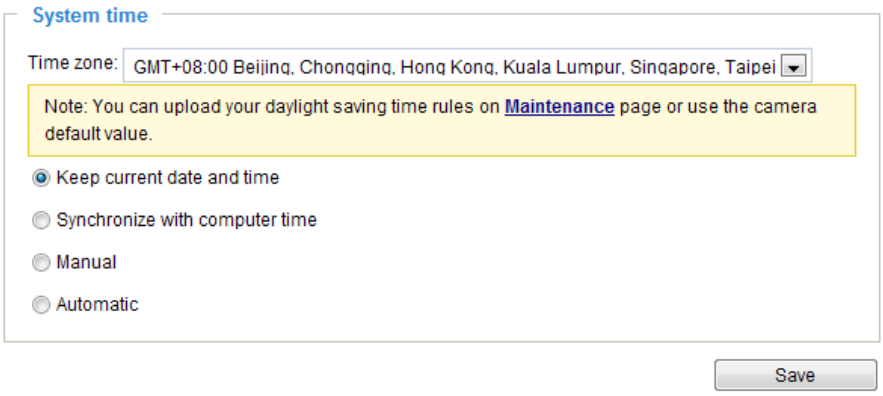
This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following two columns: System and System Time.

### System


Host name: Enter a desired name for the Network Camera. The name will be displayed at the top center of the main page.

Turn off the LED indicator: Click to disable the onboard LEDs.

## System time




Keep current date and time: Select this option to preserve the current date and time of the Network Camera. The Network Camera's internal real-time clock maintains the date and time even when the power of the system is turned off.

Sync with computer time: Select this option to synchronize the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

Manual: The administrator can enter the date and time manually. Note that the date and time format are [yyyy/mm/dd] and [hh:mm:ss].

Automatic: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically querying an NTP Server.

NTP server: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time servers.

Update interval: Select to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

Time zone Advanced Mode: Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules, please refer to **System > Maintenance > Import/ Export files** on page 50 for details.

When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

# System > Homepage layout Advanced Mode

This section explains how to set up your own customized homepage layout.

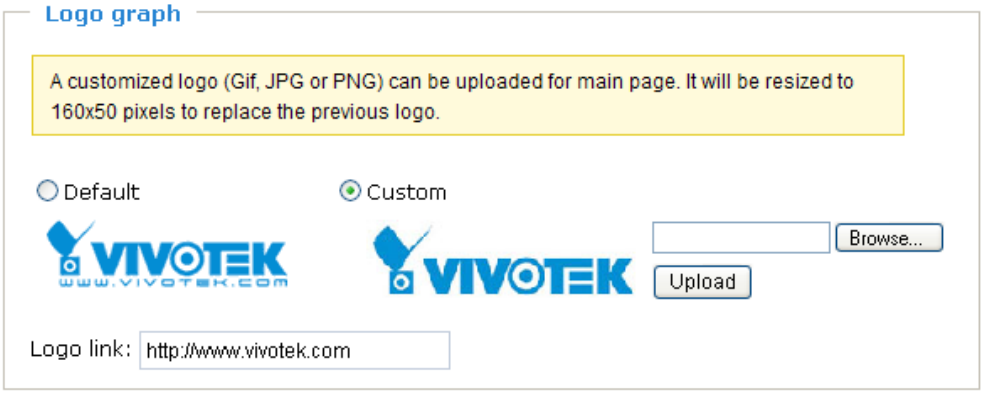
## General settings

This column shows the settings of your hompage layout. You can manually select the background and font colors in Theme Options (the second tab on this page). The settings will be displayed automatically in this Preview field. The following shows the homepage using the default settings:


■ Hide Powered by VIVOTEK: If you check this item, it will be removed from the homepage.

Logo graph

Here you can change the logo at the top of your homepage.



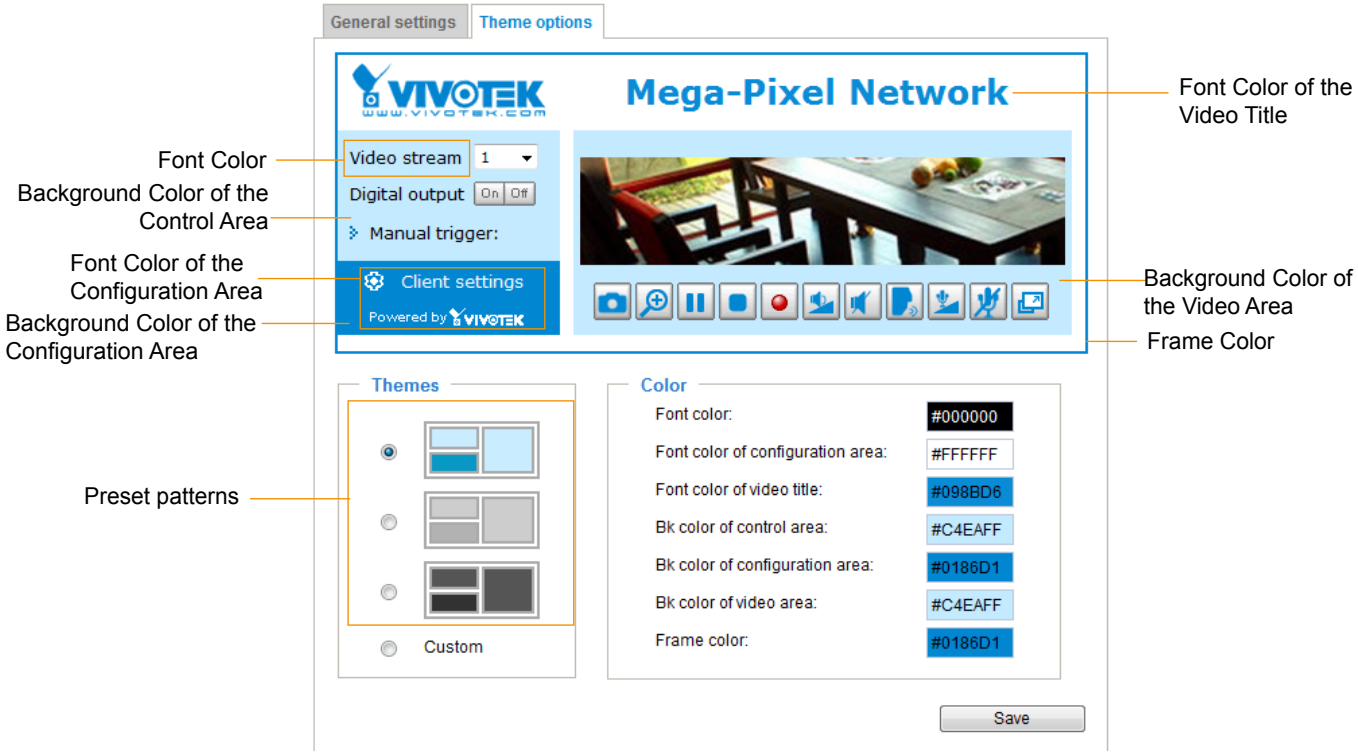

Follow the steps below to upload a new logo:
1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the settings.

Customized button

If you want to hide manual trigger buttons on the homepage, please uncheck this item. This item is checked by default.

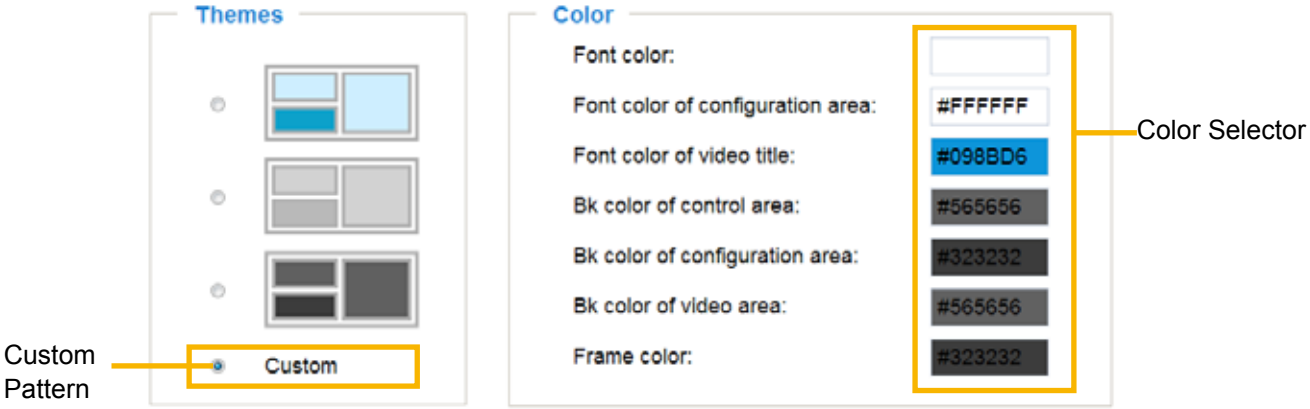
## Theme Options

Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the **Preview** filed. Click **Save** to enable the settings.

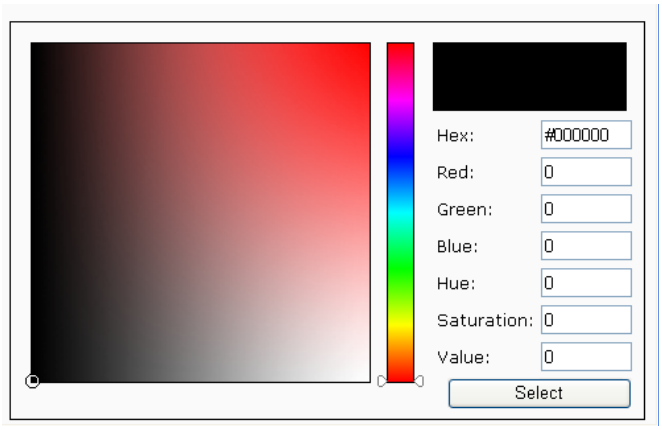




■ Follow the steps below to set up a custom homepage:
1. Click **Custom** on the left column.
2. Click to select a color on on the right column.




3. The palette window will pop up as shown below.



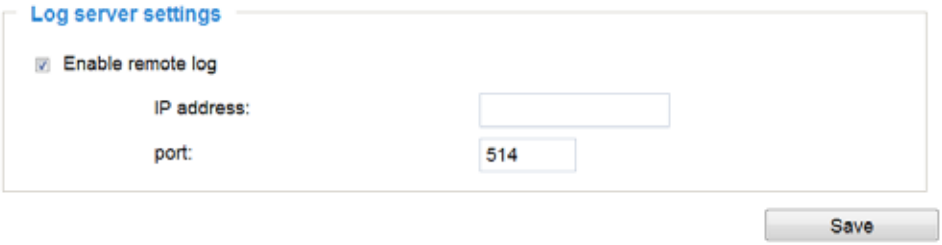


4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
6. Click **Save** to enable the settings.

# System > Logs Advanced Mode

This section explains how to configure the Network Camera to backup system log to a remote server.

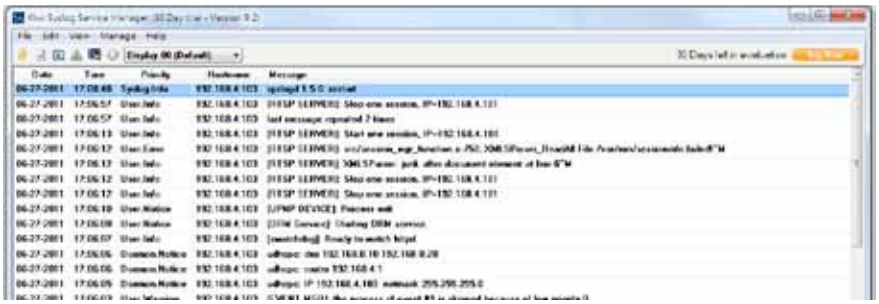
## Log server settings




Follow the steps below to set up the remote log:

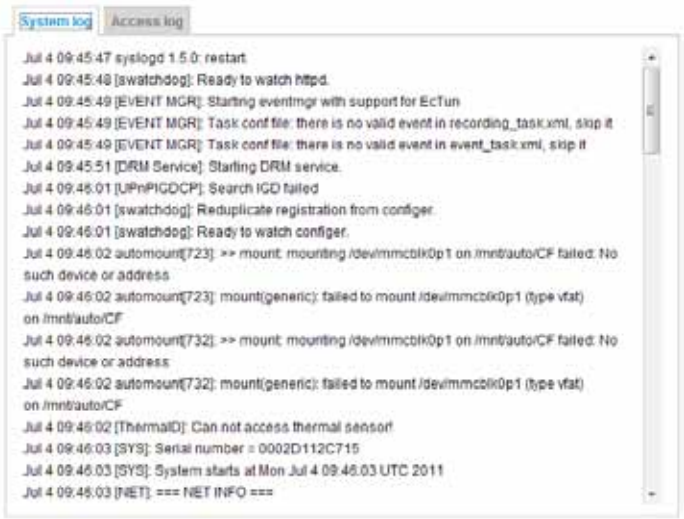
1. Select **Enable remote log**.
2. In the IP address text box, enter the IP address of the remote server.
2. In the port text box, enter the port number of the remote server.
3. When completed, click **Save** to enable the setting.

You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log messages from the Network Camera. An example is Kiwi Syslog Daemon. Visit http://www.kiwisyslog.com/kiwi-syslog-daemon-overview/.



## System log

This column displays the system log in chronological order. The system log is stored in the Network Camera's buffer and dated events will be overwritten when the number of events reaches a limit.

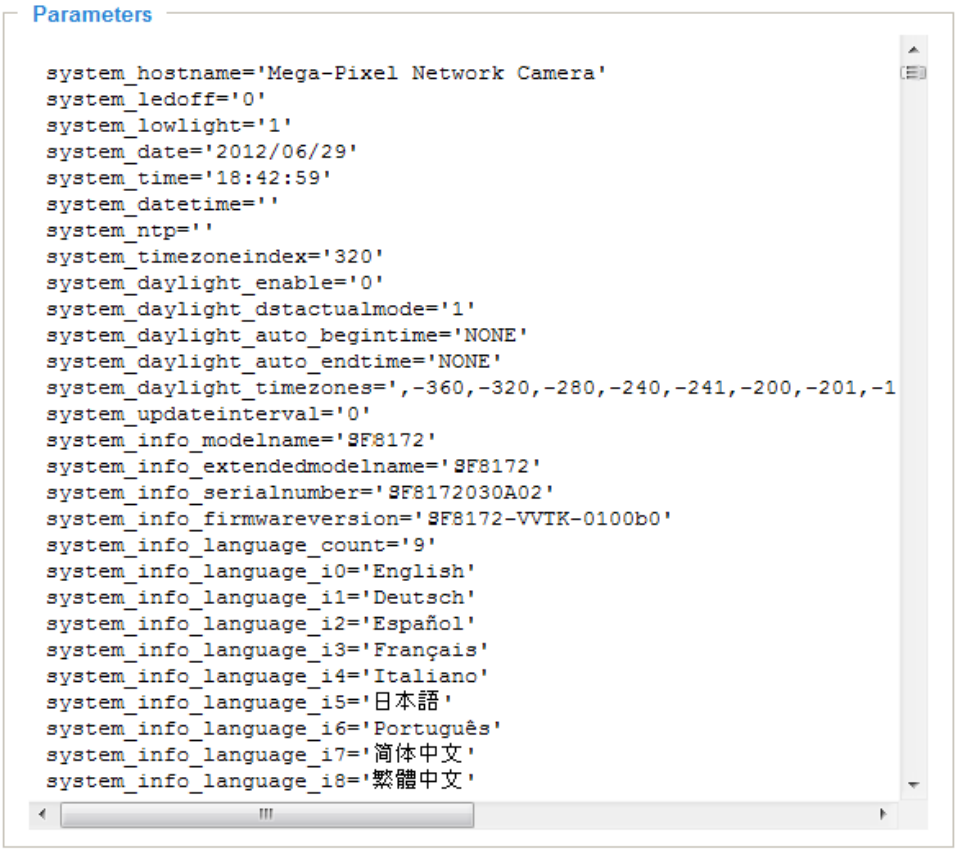


## Access log

Access log displays the access time and IP address of all viewers (including operators and administrators) in a chronological order. The access log is stored in the Network Camera's buffer and older events will be overwritten when the number of events reaches a limit.


# System > Parameters Advanced Mode

The View Parameters page lists the entire system's parameters in an alphabetical order. If you need technical assistance, use a text-editor program to copy and save the parameters listed on this page. Send the parameter text file to VIVOTEK's technical support.



# System > Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware version, etc.

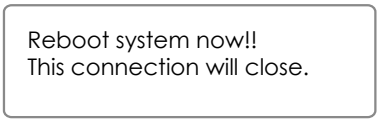
## General settings > Upgrade firmware


This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.
**Note: Do not power off the Network Camera during the upgrade!**

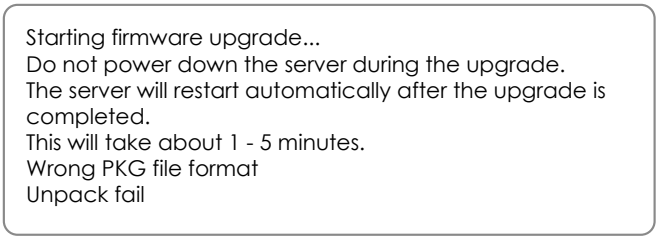
Follow the steps below to upgrade the firmware:
1. Download the latest firmware file from the VIVOTEK website. The file is in .pkg file format.
2. Click **Browse…** and specify the firmware file.
3. Click **Upgrade**. The Network Camera starts to upgrade and will reboot automatically when the upgrade completes.

If the upgrade is successful, you will see “Reboot system now!! This connection will close”. After that, re-access the Network Camera.

The following message is displayed when the upgrade has succeeded.




The following message is displayed when you have selected an incorrect firmware file.



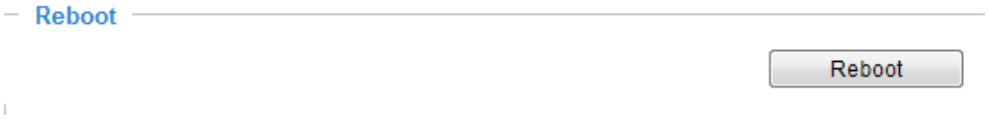

**Tips:**

If a firmware upgrade is accidentally disrupted, say, by a power outage, you still have a last resort method to restore normal operation. See the following for how to bring the camera back to work:

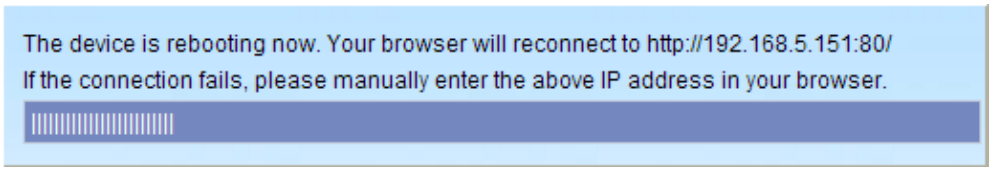
Applicable scenario:
(a) Power disconnected during FW upgrade.
(b) Unknown reason causing abnormal LED status, and a Restore cannot recover normal working condition.

You can use the following method to activate the camera with its backup firmware.
(a) Press and hold down the reset button for at least one minute.
(b) Power on the camera until the Red LED blinks rapidly.
(c) After boot up, the firmware should return to the previous version before the camera hanged. (The procedure should take 5 to 10 minutes, longer than the normal boot-up process.) When this process is completed, the LED status will return to normal.

## General settings > Reboot

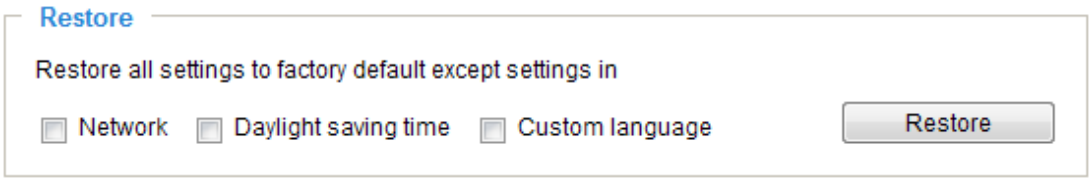



This feature allows you to reboot the Network Camera, which takes about one minute to complete. When completed, the live video page will be displayed in your browser. The following message will be displayed during the reboot process.




If the connection fails after rebooting, manually enter the IP address of the Network Camera in the address field to resume the connection.

## General settings > Restore



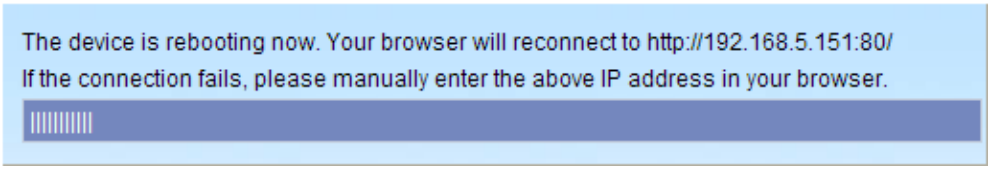

This feature allows you to restore the Network Camera to factory default settings.

Network: Select this option to retain the Network Type settings (please refer to Network Type on page 69).

Daylight Saving Time: Select this option to retain the Daylight Saving Time settings (please refer to Import/Export files below on this page).

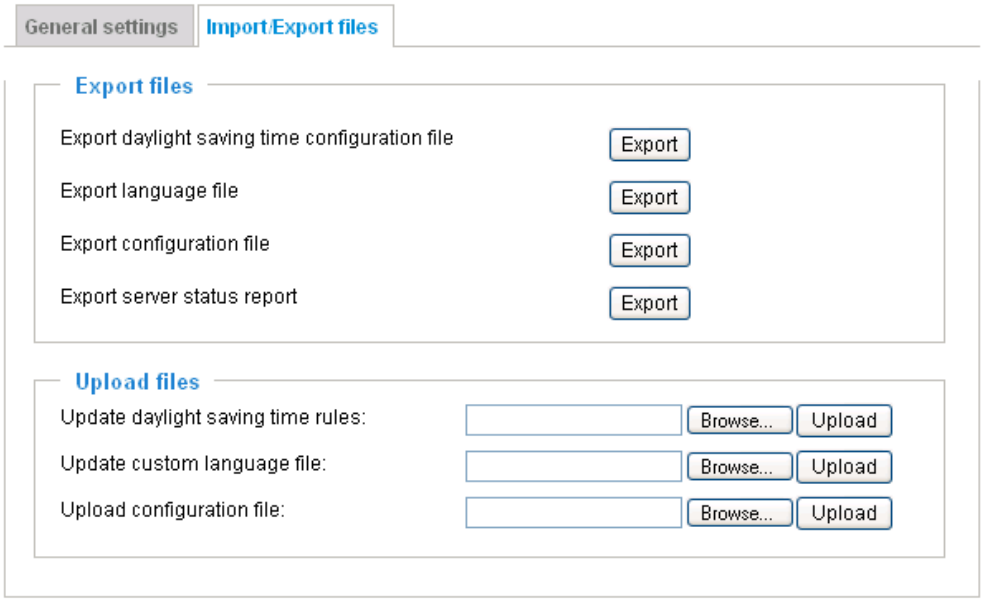
Custom Language: Select this option to retain the Custom Language settings.

If none of the options is selected, all settings will be restored to factory default. The following message is displayed during the restoring process.



## Import/Export files Advanced Mode

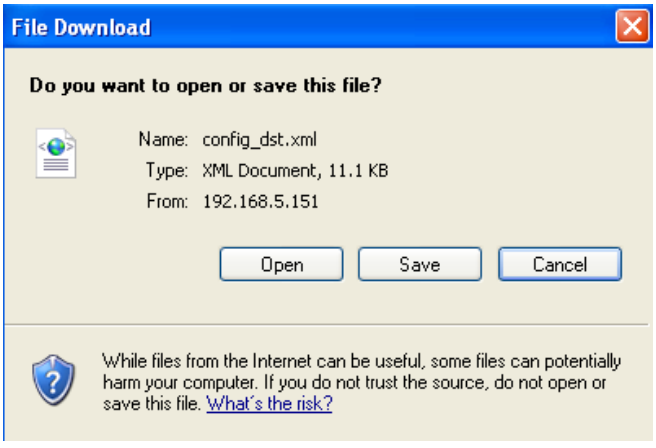
This feature allows you to Export / Update daylight saving time rules, custom language file, and configuration file.




Export daylight saving time configuration file: Click to set the start and end time of DST.

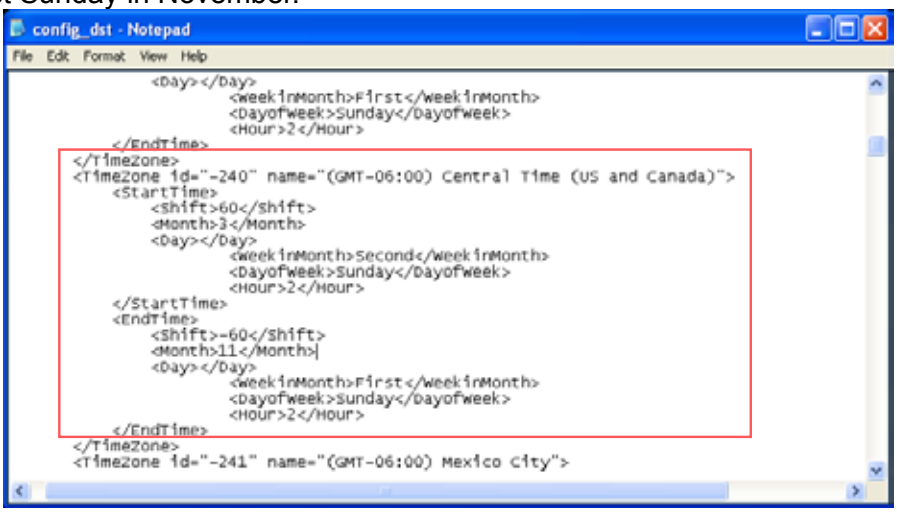
Follow the steps below to export:

1. In the Export files column, click **Export** to export the daylight saving time configuration file from the Network Camera.
2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to store the file for editing.



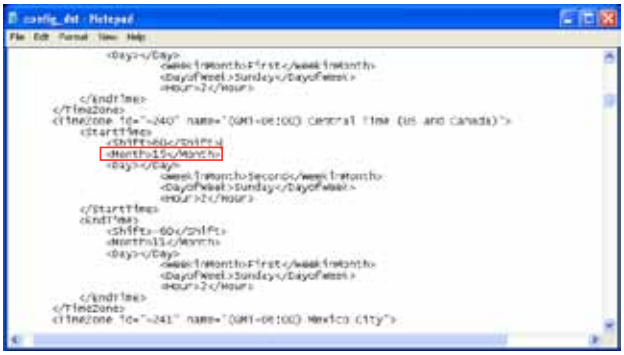
3. Open the file with Microsoft® Notepad and locate your time zone; set the start and end time of DST. When completed, save the file.

In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.

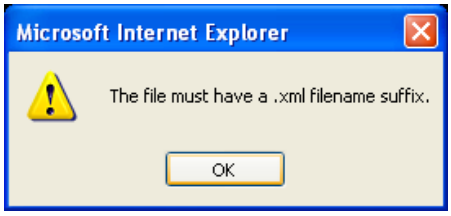



Update daylight saving time rules: Click **Browse…** and specify the XML file to update.

If incorrect date and time are assigned, you will see the following warning message when uploading the file to the Network Camera.




The following message is displayed when attempting to upload an incorrect file format.




Export language file: Click to export language strings. VIVOTEK provides nine languages: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

Update custom language file: Click **Browse…** and specify your own custom language file to upload.

Export configuration file: Click to export all parameters for the device and user-defined scripts.

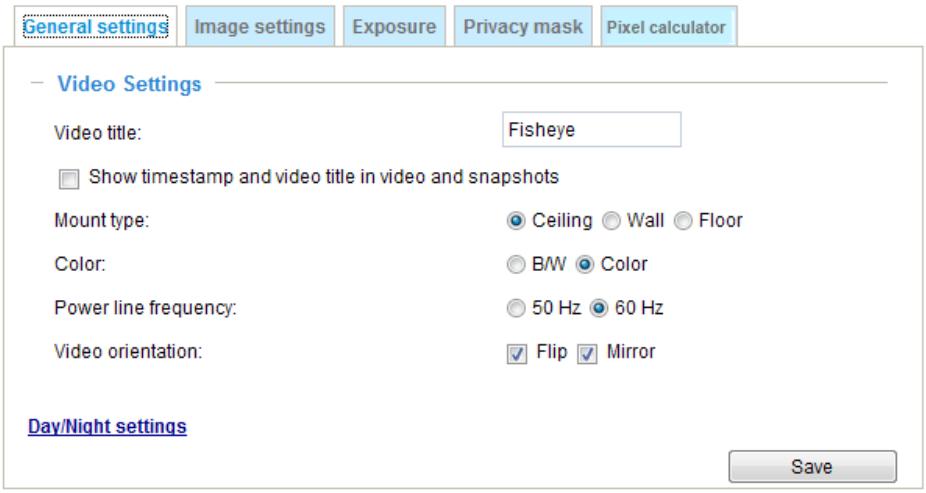
Update configuration file: Click **Browse…** to update a configuration file. Please note that the model and firmware version of the device should be the same as the configuration file. If you have set up a fixed IP or other special settings for your device, it is not suggested to update a configuration file.

Export server staus report: Click to export the current server status report, such as time, logs, parameters, process status, memory status, file system status, network status, kernel message..., and so on.

# Media > Image Advanced Mode

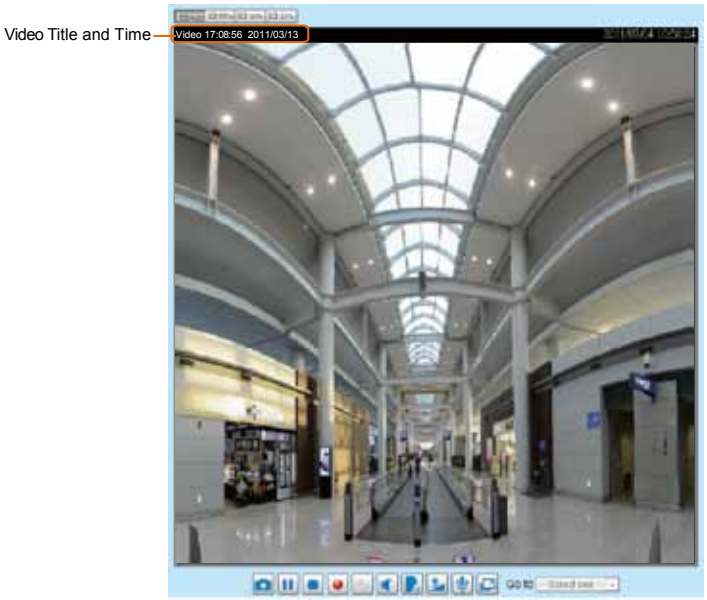
This section explains how to configure the image settings of the Network Camera. It is composed of the following tabbed windows: General settings, Image settings, Exposure, and Privacy mask, and Pixel calculator.

## General settings




Video title: Enter a name that will be displayed on the title bar of the live video as well as the view cell on the ST7501 and VAST recording software.

Show timestamp and video title in video and snapshot: Enter a name that will be displayed on the title bar of the live video as the picture shown below.




Mount type: There are 3 Mount types - Ceiling, Wall, and Floor.

**Ceiling**: The Ceiling mount type automatically delivers upside-down images.
**Wall**: The Wall mount type applies to the monitoring of long, side-to-side surveillance areas, such as a corridor. Different Mount types have effects on the Display mode settings. For example, the **1P2R** (1 Panoramic & 2 Regional) and **1P3R** (1 Panoramic & 3 Regional) Display modes are only available for the “Wall“ Mount type.
**Floor:** The Display modes with the Floor mount type are identical to those for the Ceiling mount

except that the images are not vertically flipped.

Color: Select to display color or black/white video streams.

Power line frequency: Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights.

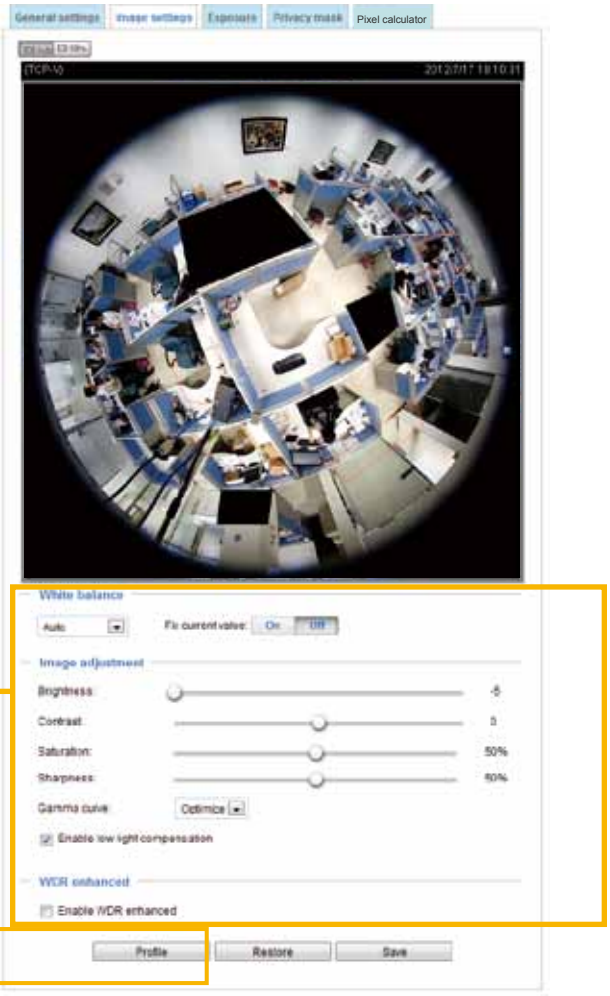
Video orientation: Flip - vertically reflect the display of the live video; Mirror - horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (e.g., on the ceiling) to correct the image orientation. Please note that the preset locations will be cleared after you configure the flip/mirror option.

## Day/Night Settings

This only provides a link to the Exposure window. See page 58 for details.

## Image settings

On this page, you can tune the White balance, Image adjustment and WDR enhanced parameters. You can configure two sets of preferred settings: one for normal situations, the other for special situations, such as day/night/schedule mode.




Sensor Setting 1:
For normal situations

Sensor Setting 2:
For special situations

White balance: Adjust the value for the best color temperature.

■ Auto: It will automatically adjust the color temperature of the light in response to different light sources. You may follow the steps below to adjust the white balance to the best color temperature.

1. Set the White balance to **Auto**.
2. Place a sheet of white paper (or a color of a cool color temperature, such as blue) in front of the lens, then allow the Network Camera to automatically adjust the color temperature.
3. Click the **Off** button on **Fix current value** to confirm the setting when the camera adjusts and measures the white balance.

■ Manual: This item allows users to manually input the R gain & B gain ratios.

Image Adjustment

■ Brightness: Adjust the image brightness level, which ranges from -5 to +5.

■ Saturation: Adjust the image saturation level, which ranges from 0% to 100%. You can also select **Customize** and manually enter a value.

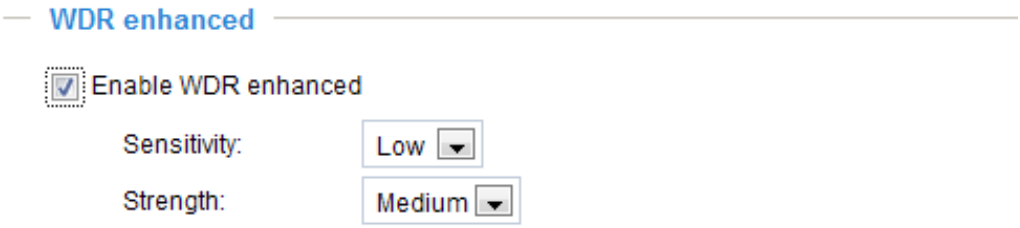
■ Contrast: Adjust the image contrast level, which ranges from -5 to +5.

■ Sharpness: Adjust the image sharpness level, which ranges from 0% to 100%.

■ Gamma curve: Gamma curve: Adjust the image sharpness level, which ranges from 0% to 100%. You may let firmware **Optimize** your display or select the **Manual** mode, and pull the slide bar pointer to change the preferred level of Gamma correction towards higher contrast or towards the higher luminance for detailed expression for both dark and lighted areas of an image.

■ Enable low light compensation: Select this option in low light mode, and the values of sharpness and brightness will change automatically. This function also benefits from an automated noise reduction feature.

WDR enhanced: This function allows users to identify more image details with an extreme contrast from an object of interest with one shadowed side against a bright background, e.g., an entrance. You may select the **Enable WDR enhanced** checkbox, and then adjust the sensitivity (low, high) and the strength (low, medium, high) to reach the best image quality.




You can click on **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the setting.

If you want to configure another sensor setting for day/night/schedule mode, please click **Profile** to open the Profile Settings page as shown below.


Please follow the steps below to setup a profile:

1. Select the **Enable and apply this profile** checkbox.
2. Select the applied mode: Day mode, Night mode, or Schedule mode. Please manually enter a range of time if you choose Schedule mode.
3. Configure the White balance and Image adjustment settings in the following columns. Please refer to the previous page for detailed information.
4. Click **Save** to enable the settings and click **Close** to exit the page.

## Exposure Advanced Mode

On this page, you can set the Exposure measurement window, Exposure level, Exposure mode, Exposure time, Gain control, and Day/Night mode settings. You can configure two sets of Exposure settings: one for normal situations, the other for special situations, such as day/night/schedule mode.


Sensor Setting 1:
For normal situations

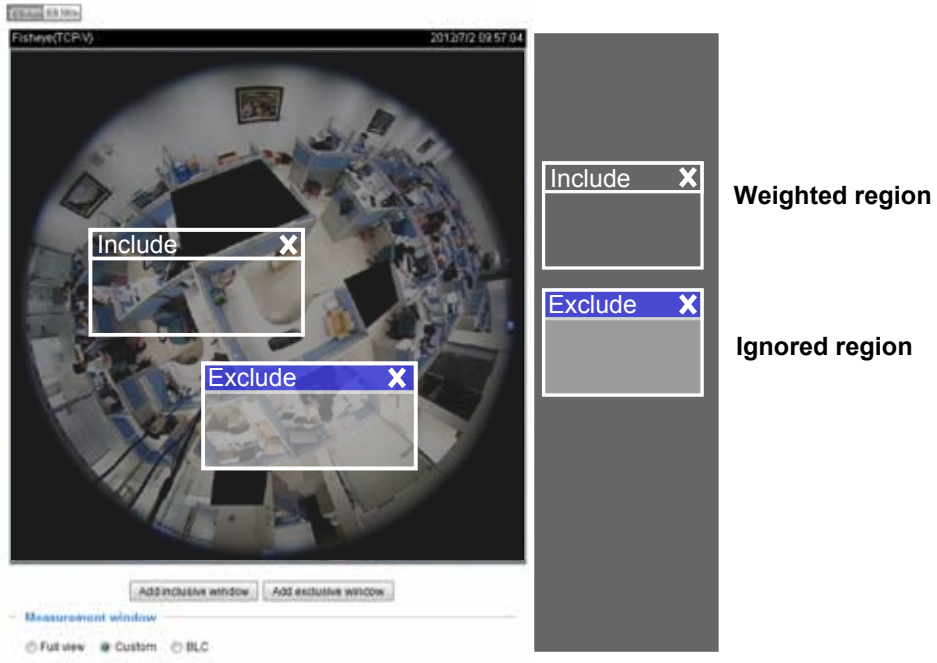
Sensor Setting 2:
For special situations

Measurement Window: This function allows users to set measurement window(s) for low light compensation. For example, where low-light objects are posed against an extremely bright background. You may want to exclude the bright sunlight shining through a building's corridor.

■ Full view: Calculate the full range of view and offer appropriate light compensation.

■ Custom: This option allows you to manually add customized windows as inclusive or exclusive regions. A total of 10 windows can be set. Please refer to the next page for detailed illustration.

The inclusive window refers to the “weighted window“; the exclusive window refers to “ignored window“. It adopts the weighted averages method to calculate the value. The inclusive windows have a higher priority. You can overlap these windows, and, if you place a exclusive window within a larger inclusive window, the exclusive part of the overlapped windows will be deducted from the inclusive window. An exposure value will then calculated out of the remaining of the inclusive window.



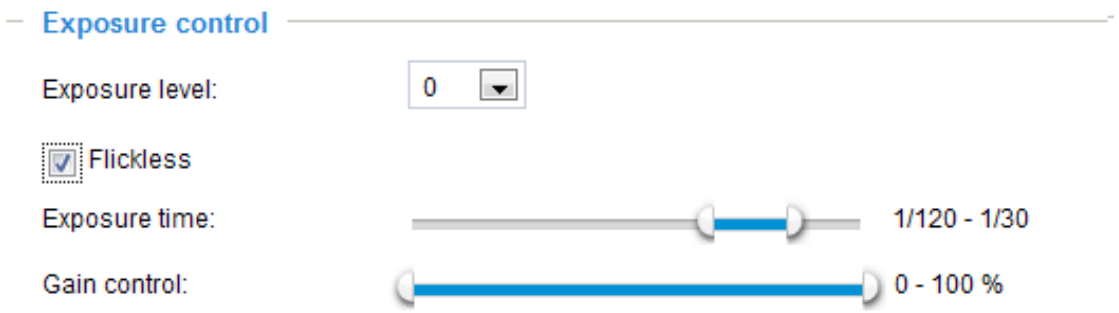

■ BLC (Back Light Compensation): This option will automatically add a “weighted region“ in the middle of the window and give the necessary light compensation.

Exposure control:

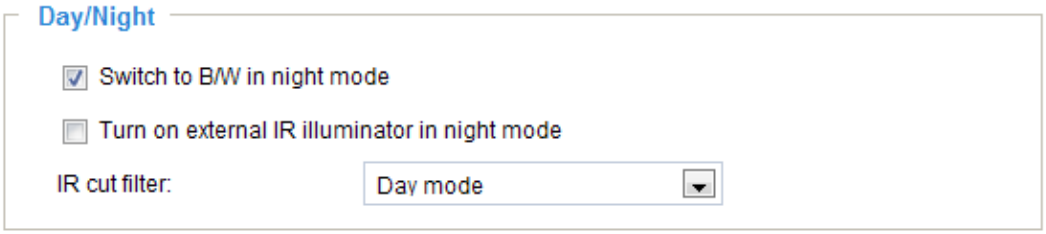
■ Exposure level: You can manually set the Exposure level, which ranges from -2.0 to +2.0 (dark to bright).

**Flickerless:** Under some circumstances when there is a differnece between the video capture frequency and local AC power frequency (NTSC or PAL), the mismatch causes color shifts or flickering images. If the above mismatch occurs, select the **Flickerless** checkbox, and the range of Exposure time (the shutter time) will be limited to a range in order to match the AC power frequency. See the screen capture below.

You can click and drag the semi-circular pointers on the **Exposure time** and **Gain control** slide bars to specify a range of shutter time and Gain control values within which the camera can automaticallly tune to an optimal imaging result. For example, you may prefer a shorter shutter time to better capture moving objects, while a faster shutter reduces light and needs to be compensated by electrical brightness gains.



## Day/Night




Switch to B/W in night mode
Select this checkbox to enable the Network Camera to automatically switch to Black & White display during the night mode.

Turn on external IR illuminator in night mode
If your camera is installed with an IR illuminator and the digital output signals are connected to it, you can let system firmware turn on the supplementary illuminator during low-light conditions.

IR cut filter
With a removable IR-cut filter, this Network Camera can automatically remove the filter to let Infrared light pass into the sensor during low light conditions.

■ Auto mode (The **Day/Night Exposure Profile** will not be available if Auto mode is selected)
The Network Camera automatically removes the filter by judging the level of ambient light.

■ Day mode
In day mode, the Network Camera switches on the IR cut filter at all times to block infrared light from reaching the sensor so that the colors will not be distorted.

■ Night mode
In night mode, the Network Camera switches off the IR cut filter at all times for the sensor to accept infrared light, thus helping to improve low light sensitivity.

■ Synchronize with digital input
The Network Camera automatically removes the IR cut filter when a digital input is triggered, for example, when the camera is accompanied by an external IR light that comes with its own sensor and provides a signal to the camera. Some camera housings come with such mechanism.

■ Schedule mode
The Network Camera switches between day mode and night mode based on a specified schedule. Enter the start and end time for day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the start and end time of day mode are set to 07:00 and 18:00.

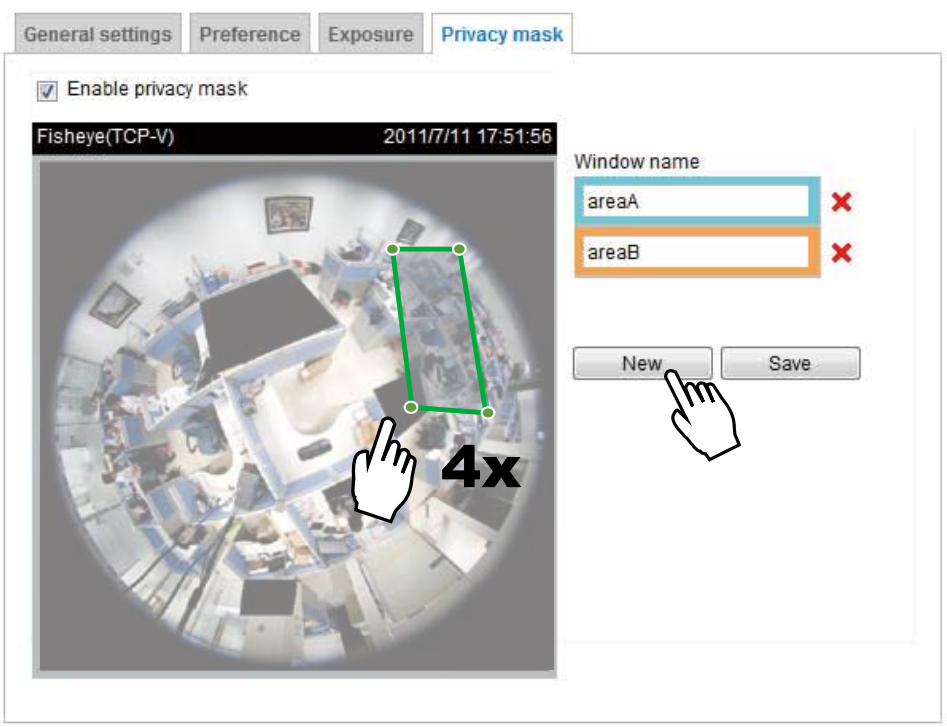
When completed with the settings on this page, click **Save** to enable the settings.

If you want to configure another sensor setting for day/night/schedule mode, please click **Profile** to open the Profile settings page as shown below.

Please follow the steps below to setup a profile:
1. Check **Enable and apply this profile**.
2. Select the applied mode: **Day mode**, **Night mode**, or **Schedule mode**. Please manually enter a range of time through which you want the Schedule mode to apply.
3. Configure Exposure control settings in the folowing columns. Please refer to the previous page for detailed information.
4. Click **Save** to enable the setting and click **Close** to exit the window.

## Privacy mask Advanced Mode

Click **Privacy Mask** to open the settings page. On this page, you can block out certain sensitive zones to address privacy concerns.




■ To set the privacy mask windows, follow the steps below:

1. Click **New** to add a new window. A text box will appear allowing you to enter a name for the mask.
2. Use four mouse clicks to mark a square area, which is recommended to be at least twice the size of the object (height and width) you want to cover.
3. Enter a Window Name and click **Save** to enable the setting.
4. Check **Enable privacy mask** to enable this function.

**NOTE:**

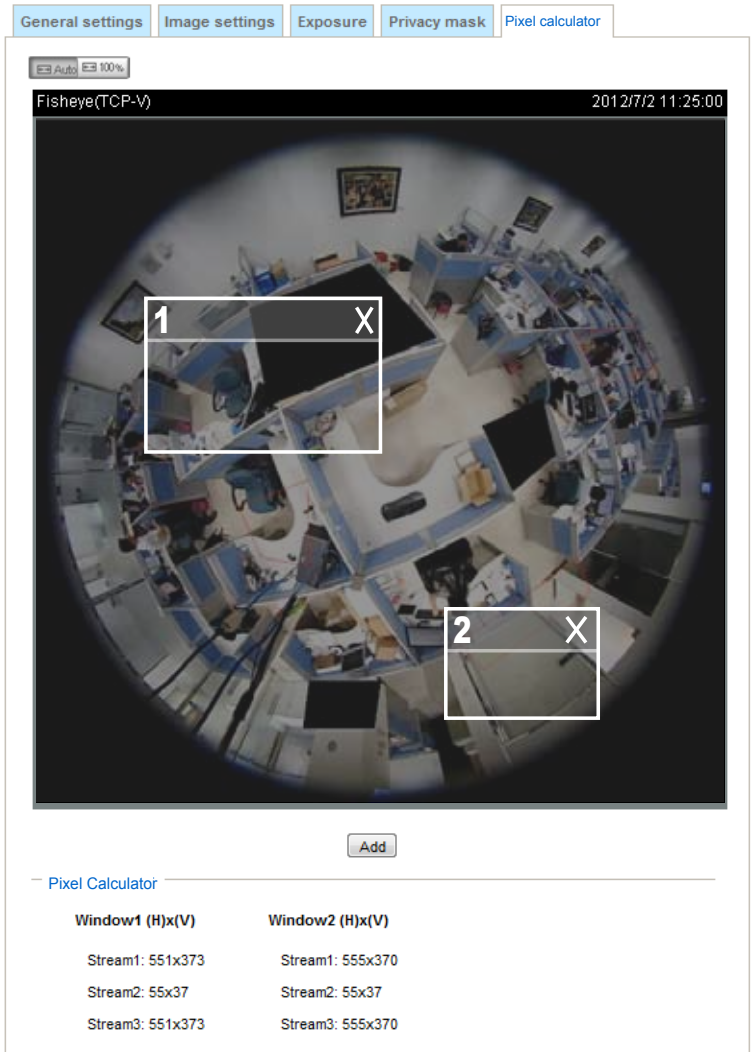
► *Up to 5 privacy mask windows can be configured on the same screen.*

► To delete a mask, use the red cross button and then click on the **Save** button.

## Pixel calculator Advanced Mode

Click the Add button at the lower screen to create a pixel calculation window. Place your cursor on the window to move it to an area of your interest, and change the size of window to fit the area of interest.

Once they are drawn, the numbers of pixels of the sides of windows will appear. This allows you to calculate if your current configuration fulfills a requirement, for instance, recognizing the faces of persons passing through a location. A facial recognition usually requires around 130 pixels per meter or higher.



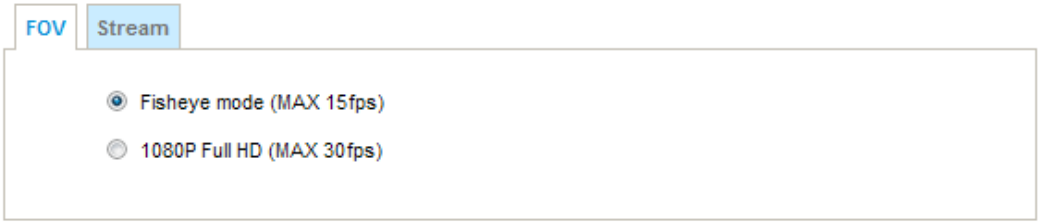

The pixels thus calculated is listed at the lower screen on a per-stream basis depending on the frame size you configure for each video stream.

# Media > Video

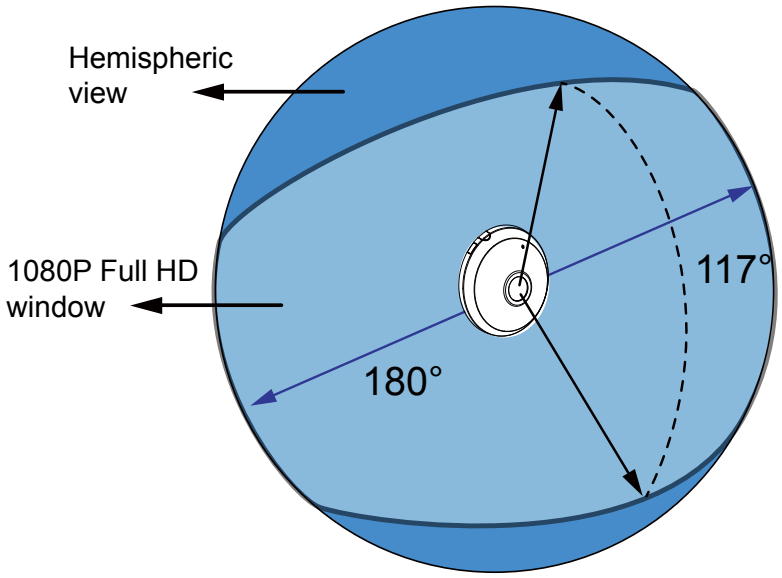
## FOV Advanced Mode

The Field of View window allows you to select either the Fisheye mode or a 1080P Full HD mode. The 1080P Full HD mode provides a dewarpped section (1920x1080 pixels) out of the 180 degrees hemispheric view. The 1080P Full HD mode provides a higher frame rate of up to 30fps. It is as if using the fisheye camera as a standard fixed dome camera.

In the 1080P Full HD mode, regional and panoramic view modes are not available. Also, changing the FOV option will erase the motion detection, privacy mask, and preset postions you previously configured.

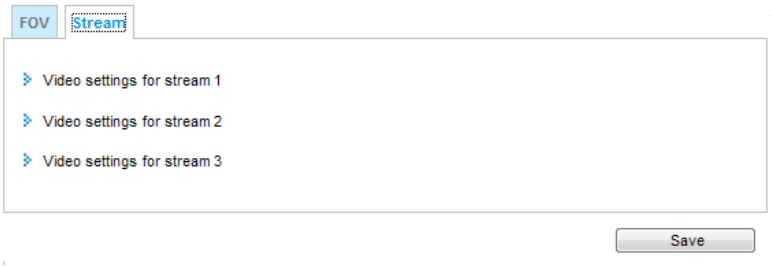



Below is a conceptual drawing showing the coverage of the 1080P Full HD mode.



## Stream settings

Advanced Mode




This Network Camera supports multiple streams with frame size ranging from 192 x 192 to 1920 x 1920.

Please follow the steps below to set up those settings for an individual stream:
1. Select a stream to configure its viewing region.
2. Choose a proper **Frame Size** from the drop-down list according to the size of monitored device.
3. Select the Maximum frame rate.

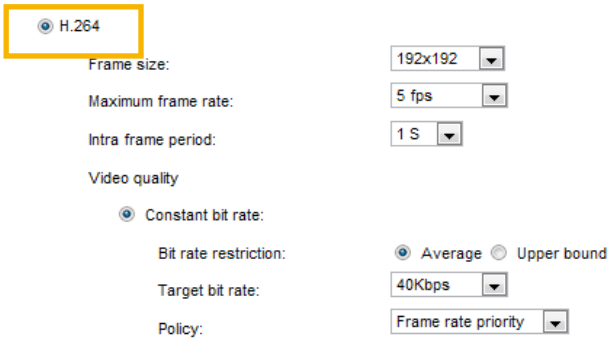
■ The parameters of the multiple streams:

| | Frame size |
|---|---|
| Stream 1 | 1920 X 1920 ~ 192 x 192 (Selectable) |
| Stream 2 | 1920 X 1920 ~ 192 x 192 (Selectable) |
| Stream 3 | 1920 X 1920 ~ 192 x 192 (Selectable) |

To change frame size, frame rate, and other related settings, click on video settings for a video stream to its individual configuration panel.

Click the stream item to display the detailed information.


This Network Camera offers real-time SVC, H.264, MPEG-4 and MJPEG compression standards (Triple Codec) for real-time viewing.
If **H.264** or **MPEG-4** mode is selected, the video is streamed via RTSP protocol. There are four parameters for you to adjust the video performance:




■ Frame size
You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

■ Maximum frame rate
This limits the maximum refresh frame rate per second. Set the frame rate higher for smoothlier video quality.
Regardless of the power line frequency setting (60Hz or 50Hz), the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, and 15fps. You can also select **Customize** and manually enter a value.

■ Intra frame period
Determine how often to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

■ Video quality
A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. Therefore, if **Constant bit rate** is selected, the bandwidth utilization is fixed at a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, 4Mbps, 6Mbps, 8Mbps, 10Mbps, 12Mbps, 14Mbps, and 16Mbps. You can also select **Customize** and manually enter a value.

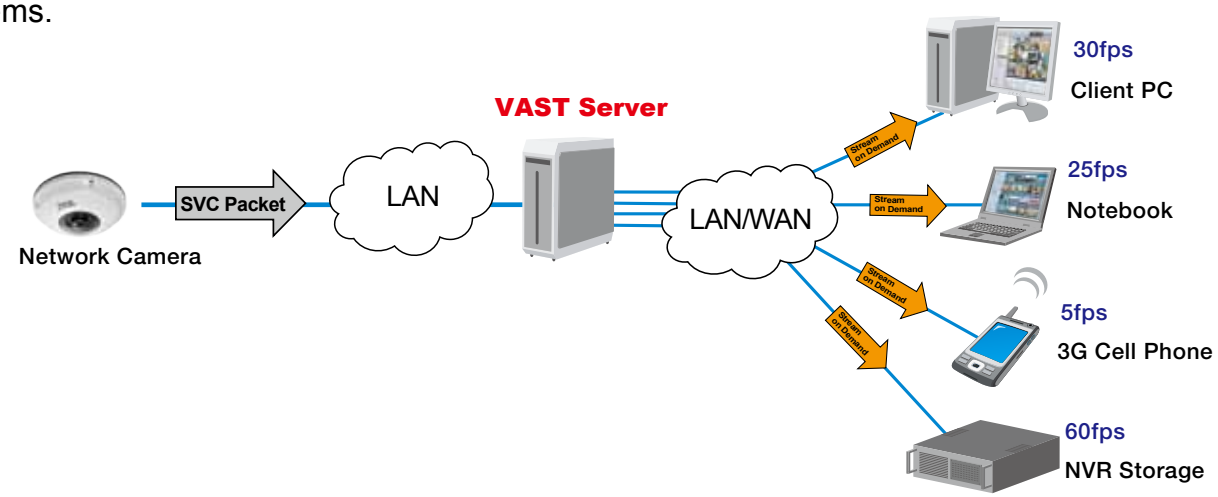
**Bit rate restriction**: The bit rate configuration is characterized either by the **Average** or the **Upper bound** approaches: the target bit rate utilized can be fluctuating around an average bit rate value or using the bit rate value as an Upper bound threshold.

**Policy**: You may select Frame rate priority or Image quality priority. The firmware dynamically controls bit rate and image quality to maintain the frame rate. If quality priority is selected, frame rate will be slightly compromized.

On the other hand, if **Fixed quality** is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

## SVC

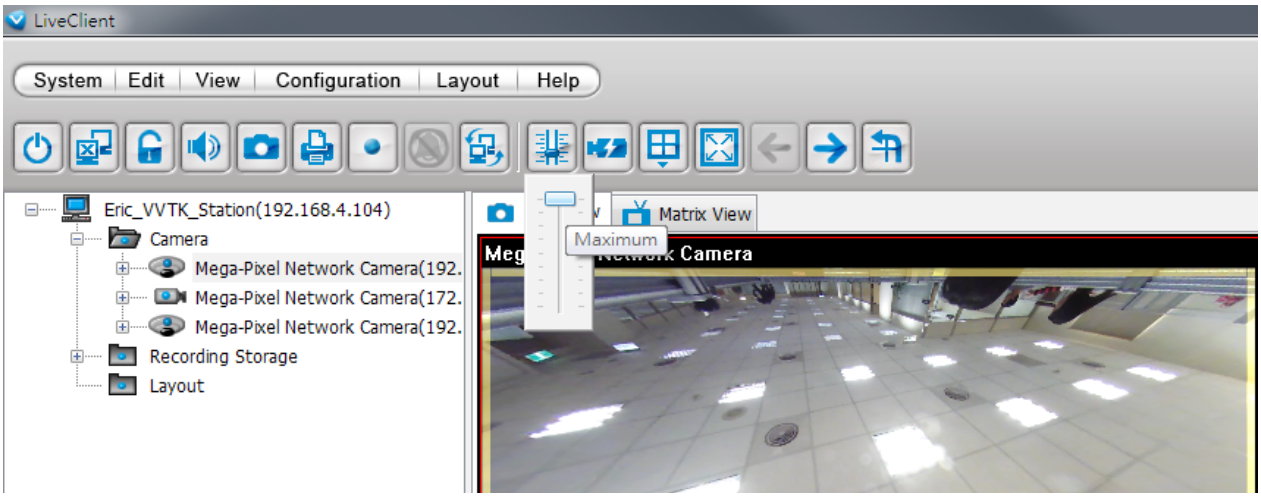
The SVC (Scalable Video Coding) feature enables streaming of videos for multiple clients from one single set of layered IP packets. Designed for saving bandwidth and CPU load on client stations, the frame rate of a video stream appearing through a view cell can be individually adjusted. This feature applies when an administrator experiences unstable video streaming due to the lack of network bandwidth, less-than-ideal hardware, or during an occurence of network problems.



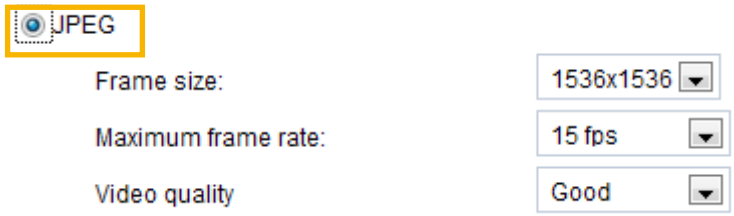

VIVOTEK's VAST server (rev. 1.6.1 and later) automatically negotiates with a camera and determines whether a network camera comes with the SVC feature. The SVC checkbox appears if the network camera supports the feature. The same checkbox also appears in the Batch Insert Cameras window. Note that the maximum frame rate varies with different cameras.

The rest of the video configuration options in the SVC column is identical to that of the H.264 protocol.

A sample screen of an SVC configuration option on a VAST LiveClient session is shown below:




If **JPEG** mode is selected, the Network Camera continuously sends JPEG images to the client, producing a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. Because the media contents are a combination of JPEG images, no audio data is transmitted to the client. There are three parameters provided in MJPEG mode to control the video performance:




■ Frame size
You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

■ Maximum frame rate
This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality.
The frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, and 15fps. You can also select **Customize** and manually enter a value. The frame rate will decrease if you select a higher resolution.

■ Video quality
The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

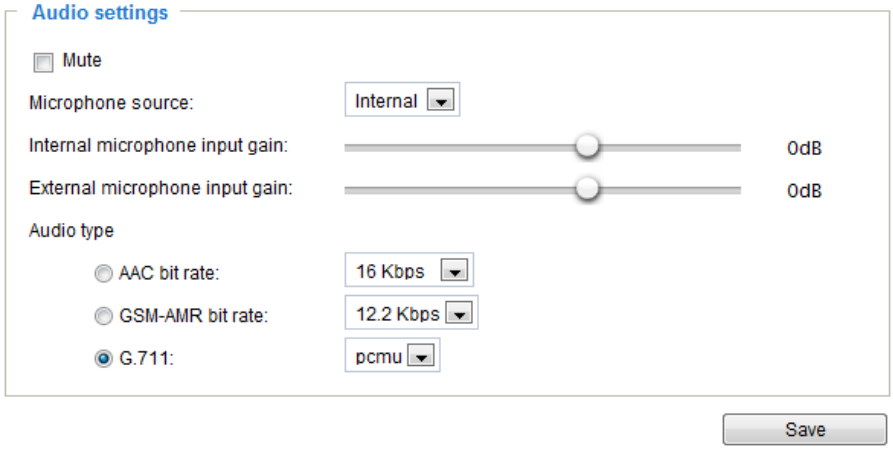
**NOTE:**

► *Video quality and fixed quality refers to the compression rate. If you select to enter a Customized value in the Fixed quality menu, a lower value will produce higher quality.*

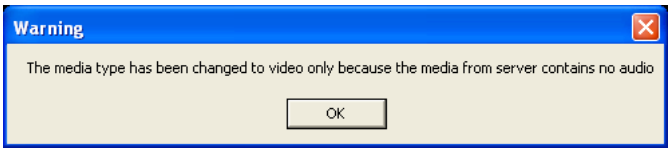
► *Converting high-quality video may significantly increase the CPU loading, and you may encounter streaming disconnection or video loss while capturing a complicated scene. In the event of occurance, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.*

# Media > Audio

## Audio Settings




Mute: Select this option to disable audio transmission from the Network Camera to all clients. Note that if mute mode is turned on, no audio data will be transmitted even if audio transmission is enabled on the Client Settings page. In that case, the following message is displayed:




Internal microphone input gain: Select the gain of the internal audio input according to ambient conditions. Adjust the gain from -33dB (least) to 21dB (most).
External microphone input gain: Select the gain of the external audio input according to ambient conditions. Adjust the gain from -33dB (least) to 21dB (most).

Audio type: Select audio codec AAC, GSM-AMR, or G.711 and the bit rate.

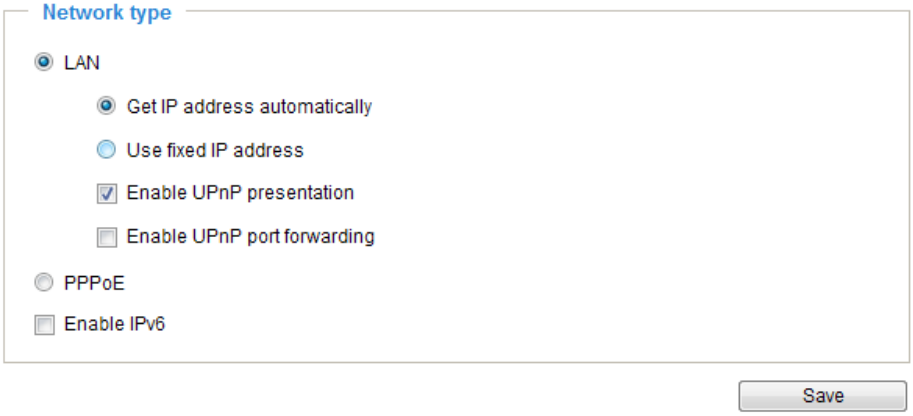
- AAC provides good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable from: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps, and 128Kbps.
- GSM-ARM is designed to optimize speech quality and requires less bandwidth. The bit rates are selectable from: 4.75Kbps, 5.15Kbps, 5.90Kbps, 6.7Kbps, 7.4Kbps, 7.95Kbps, 10.2Kbps, and 12.2Kbps.
- G.711 also provides good sound quality and requires about 64Kbps. Select pcmu (μ-Law) or pcma (A-Law) mode.

When completed with the settings on this page, click **Save** to enable the settings.

# Network > General settings

This section explains how to configure a wired network connection for the Network Camera.

## Network Type

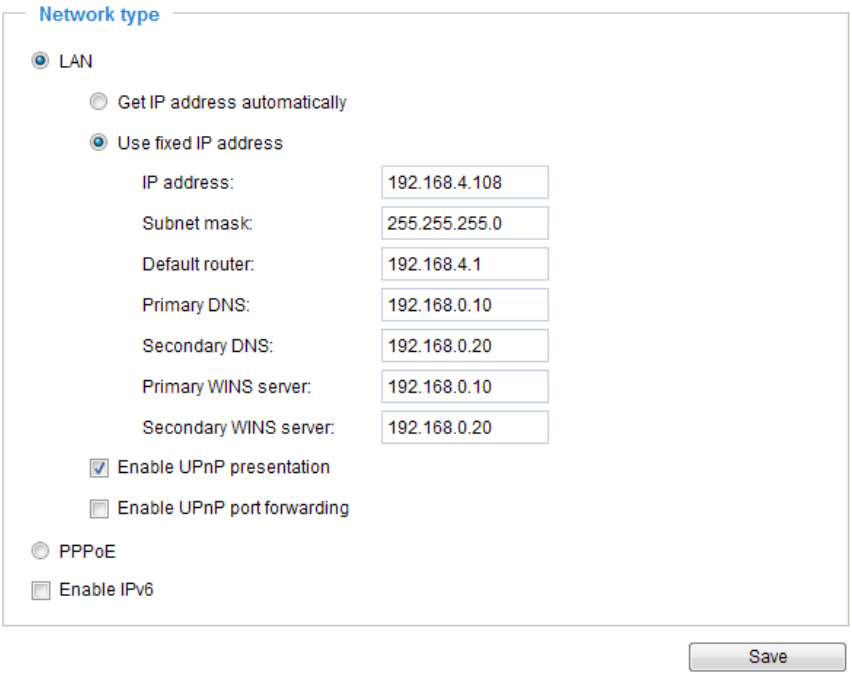



### LAN

Select this option when the Network Camera is deployed on a local area network (LAN) and is intended to be accessed by local computers. The default setting for the Network Type is LAN. Rememer to click **Save** when you complete the Network setting.

Get IP address automatically: Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the Network Camera.




1. You can make use of VIVOTEK Installation Wizard 2 on the software CD to easily set up the Network Camera on LAN. Please refer to Software Installation on page 21 for details.
2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP.

Subnet mask: This is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.

Default router: This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will fail the transmission to destinations in different subnet.

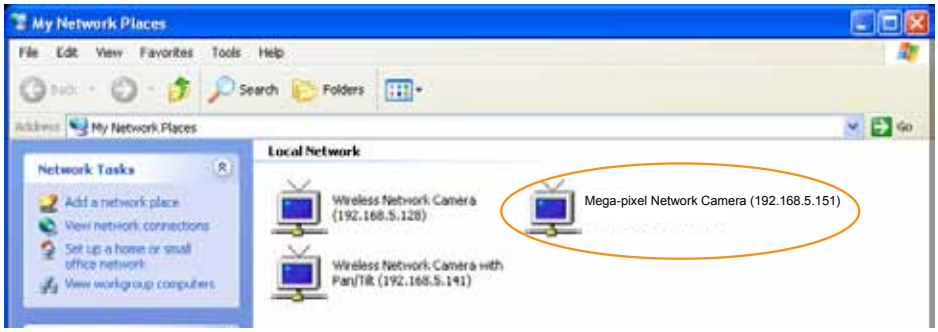
Primary DNS: The primary domain name server that translates hostnames into IP addresses.

Secondary DNS: Secondary domain name server that backups the Primary DNS.

Primary WINS server: The primary WINS server that maintains the database of computer name and IP address.

Secondary WINS server: The secondary WINS server that maintains the database of computer name and IP address.

Enable UPnP presentation: Select this option to enable UPnP™ presentation for your Network Camera so that whenever a Network Camera is presented to the LAN, shortcuts of connected Network Cameras will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently, UPnP™ is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP™ component is installed on your computer.



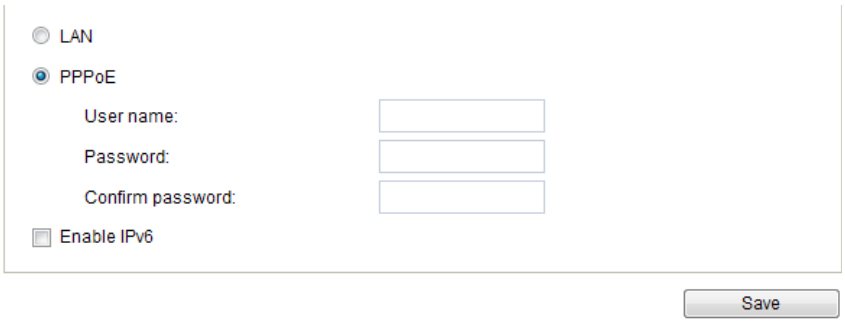

Enable UPnP port forwarding: To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports on the router automatically so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnP™ and it is activated.

## PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.

1. Set up the Network Camera on the LAN.
2. Go to Configuration > Event > Event settings > Add server (please refer to Add server on page 107) to add a new email or FTP server.
3. Go to Configuration > Event > Event settings > Add media (please refer to Add media on page 111). Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
4. Go to Configuration > Network > General settings > Network type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.




5. The Network Camera will reboot.
6. Disconnect the power to the Network Camera; remove it from the LAN environment.

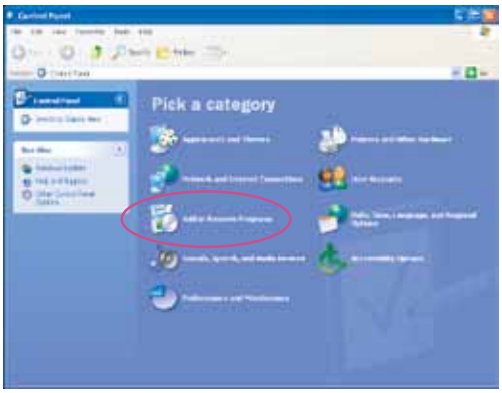
**NOTE:**

► *If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.*

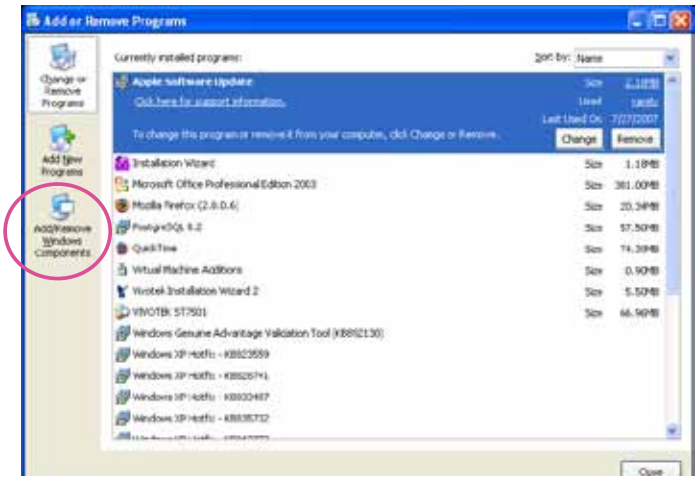
► *If UPnP™ is not supported by your router, you will see the following message:*
***Error: Router does not support UPnP port forwarding.***

► *Below are steps to enable the UPnP™ user interface on your computer:*
*Note that you must log on to the computer as a system administrator to install the UPnP™ components.*

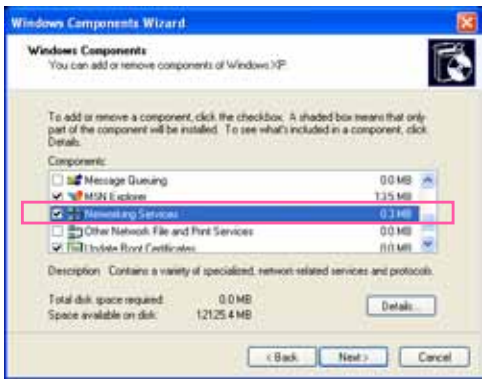
*1. Go to Start, click **Control Panel**, then click **Add or Remove Programs**.*



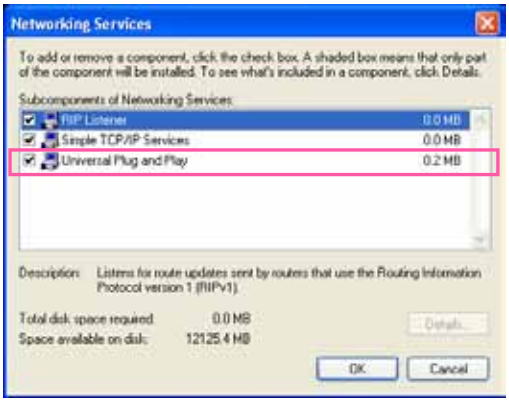

*2. In the Add or Remove Programs dialog box, click **Add/Remove Windows Components**.*



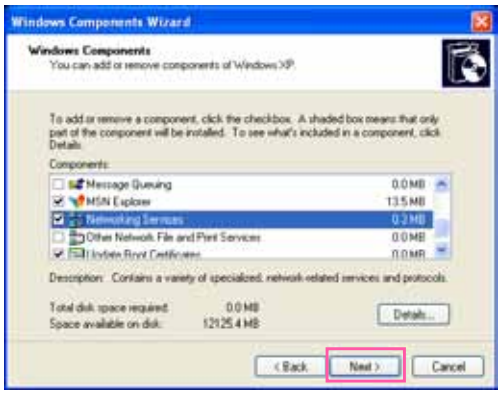

*3. In the Windows Components Wizard dialog box, select **Networking Services** and click **Details**.*



4. In the Networking Services dialog box, select ***Universal Plug and Play*** and click ***OK***.




5. Click ***Next*** in the following window.




6. Click ***Finish***. UPnP™ is enabled.

► *How does UPnP™ work?*
*UPnP™ networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts under My Network Places.*

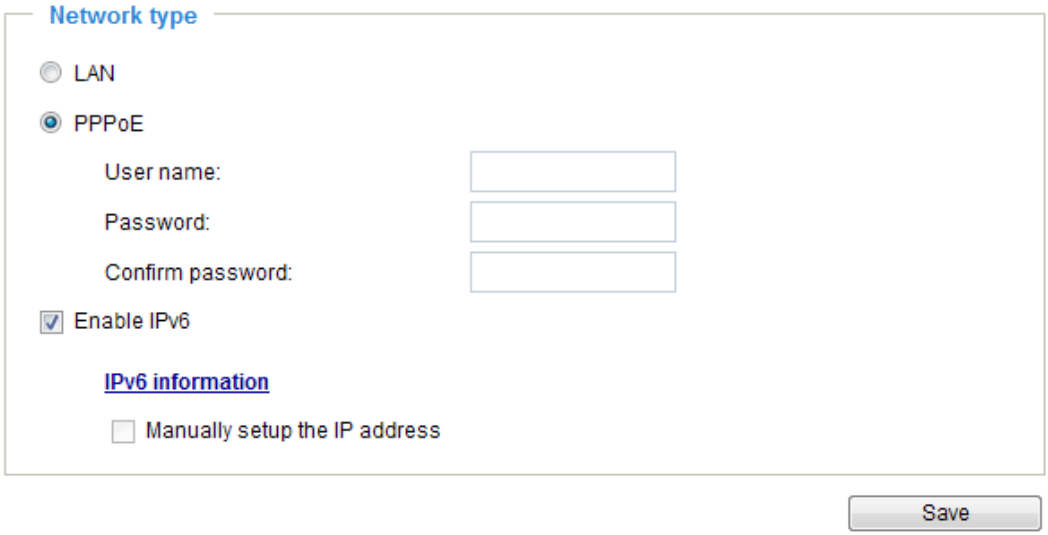
► *Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.*

| From the Internet | In LAN |
|---|---|
| http://203.67.124.123:8080 | http://192.168.4.160 or<br>http://192.168.4.160:8080 |

► *If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to* ***Restore*** *on page 50 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.*

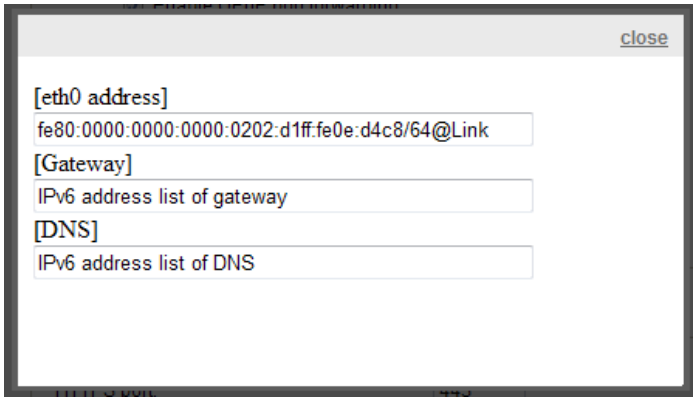
## Enable IPv6

Select this option and click **Save** to enable IPv6 settings.
Please note that this only works if your network environment and hardware equipment support IPv6. The browser should be Microsoft® Internet Explorer 6.5, Mozilla Firefox 3.0 or above.

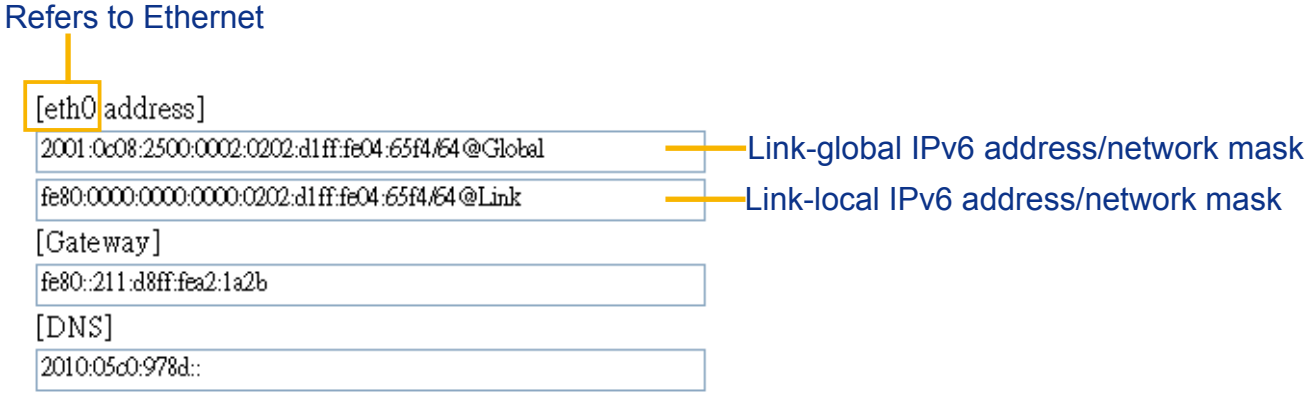



When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

IPv6 Information: Click this button to obtain the IPv6 information as shown below.

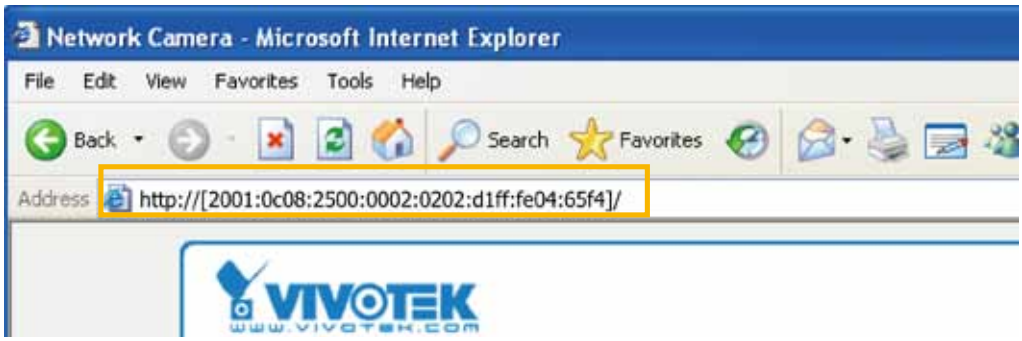



If your IPv6 settings are successful, the IPv6 address list will be listed in the pop-up window. The IPv6 address will be displayed as follows:



Please follow the steps below to link to an IPv6 address:
1. Open your web browser.
2. Enter the link-global or link-local IPv6 address in the address bar of your web browser.
3. The format should be:

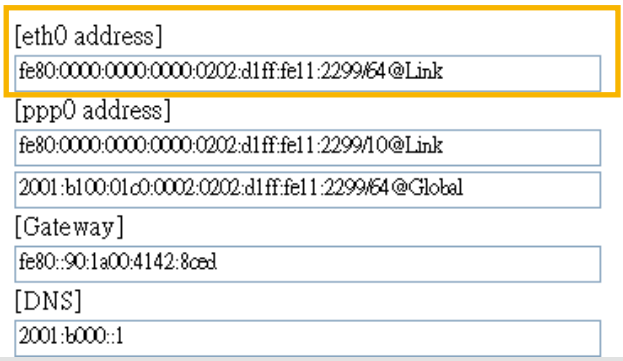

4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.
For example:



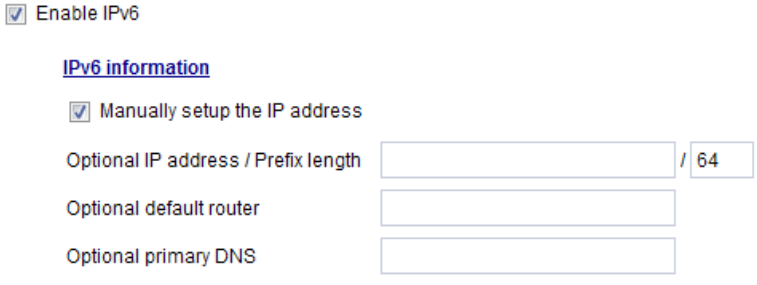

**NOTE:**

► *If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage in the following address format: (Please refer to **HTTP** streaming on page 77 for detailed information.)*

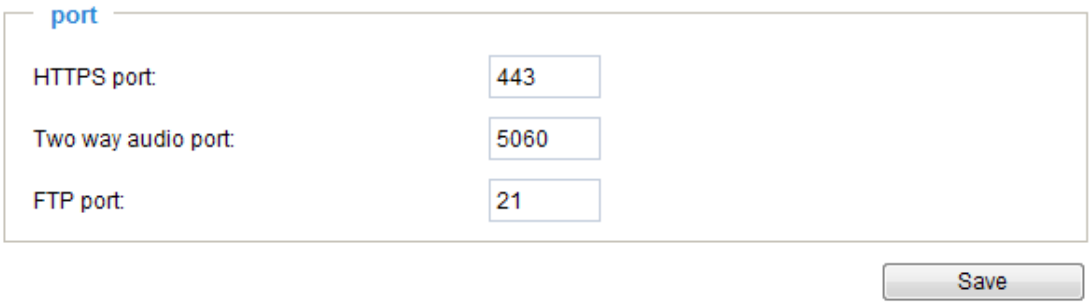

► *If you choose PPPoE as the Network Type, the [PPP0 address] will be displayed in the IPv6 information column as shown below.*




Manually setup the IP address: Select this option to manually set up IPv6 settings if your network environment does not have DHCPv6 server and router advertisements-enabled routers.
If you check this item, the following blanks will be displayed for you to enter the corresponding information:



## Port

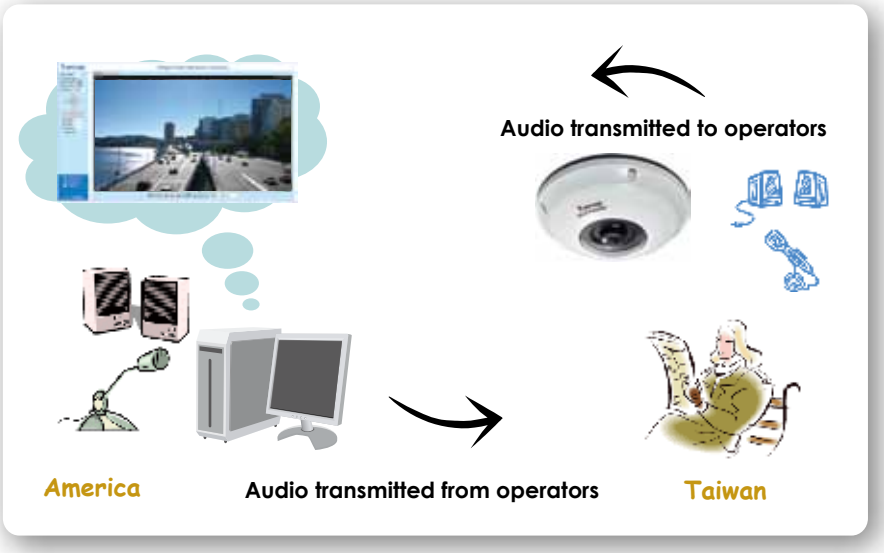


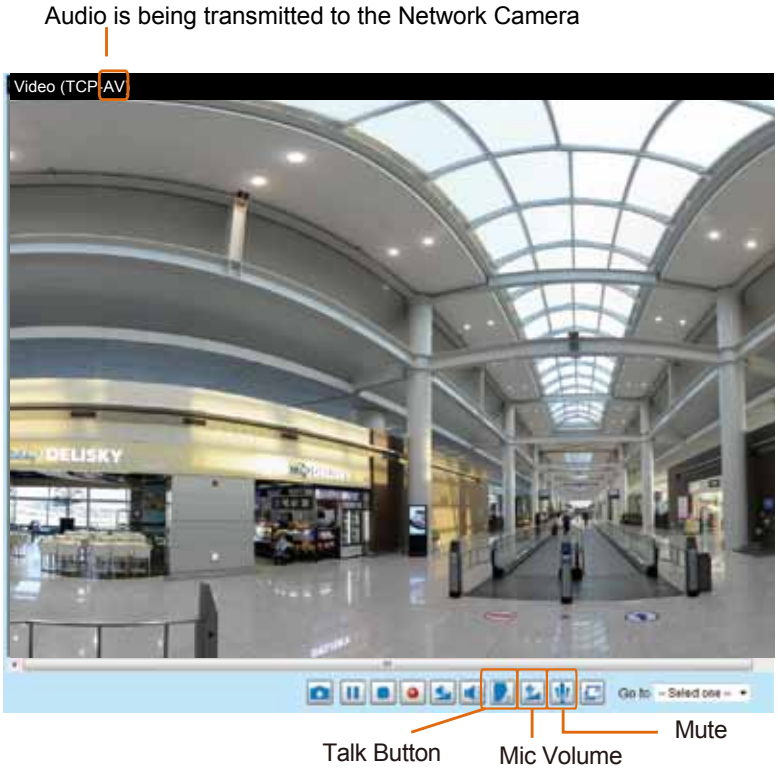

HTTPS port: By default, the HTTPS port is set to 443. It can also be assigned to another port number between 1025 and 65535.

Two way audio port: By default, the two way audio port is set to 5060. Also, it can also be assigned to another port number between 1025 and 65535.

The Network Camera supports two way audio communication so that operators can transmit and receive audio simultaneously. By using the Network Camera's built-in or external microphone and an external speaker, you can communicate with people around the Network Camera.

Note that as JPEG only transmits a series of JPEG images to the client, to enable the two-way audio function, make sure the video mode is set to "MPEG-4" or "H.264" on the Media > Video > Stream settings page and the media option is set to "Media > Video > Stream settings" on the Client Settings page. Please refer to Client Settings on page 39 and Stream settings on page 64.





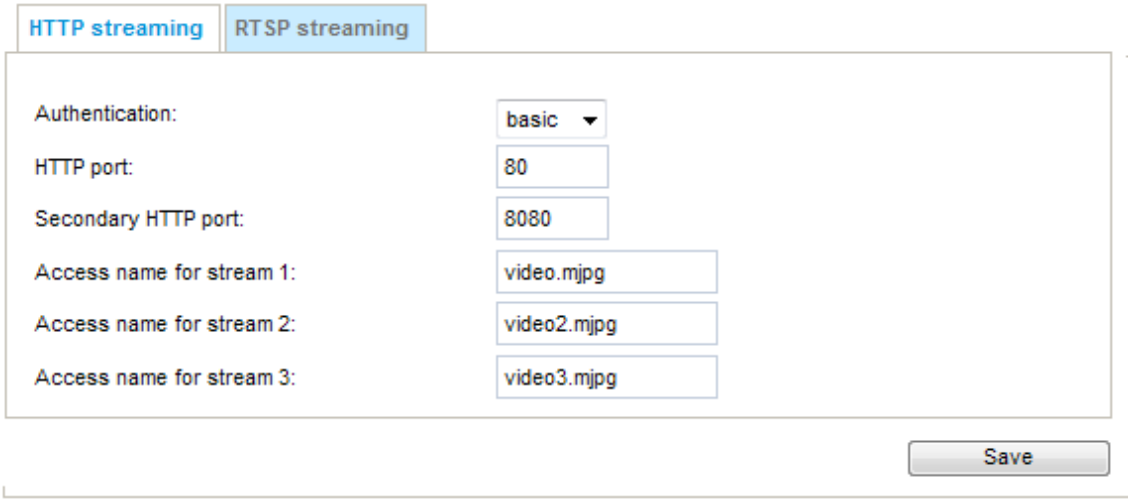

Click  to enable audio transmission to the Network Camera; click  to adjust the volume of microphone; click  to turn off the audio. To stop talking, click  again.

FTP port: The FTP server allows the user to save recorded video clips. You can utilize VIVOTEK's Installation Wizard 2 to upgrade the firmware via FTP server. By default, the FTP port is set to 21, or assigned to another port number between 1025 and 65535.

# Network > Streaming protocols Advanced Mode

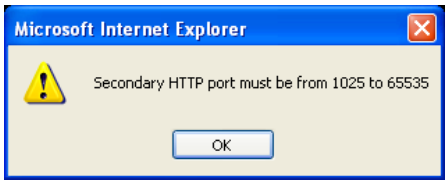
## HTTP streaming

To utilize HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security > User account on page 88 for details.




Authentication: Depending on your network security requirements, the Network Camera provides two types of security settings for an HTTP transaction: basic and digest.
If **basic** authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide better protection against unauthorized accesses.

HTTP port / Secondary HTTP port: By default, the HTTP port is set to **80** and the secondary HTTP port is set to **8080**. They can also be assigned to another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages will be displayed:

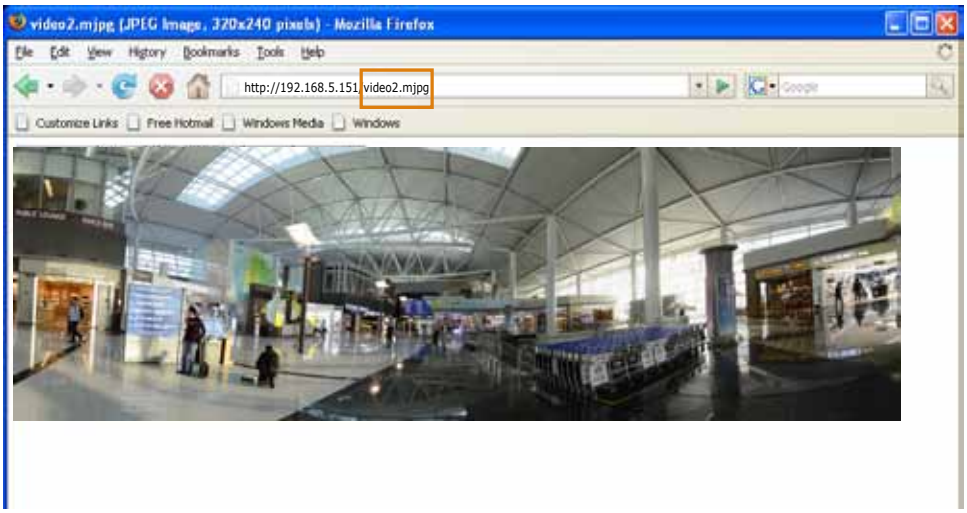

To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

| On the LAN |
| --- |
| http://192.168.4.160 or<br>http://192.168.4.160:8080 |

Access name for stream 1 ~ 3: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. Users can click **Media > Video > Stream settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Stream settings on page 64.

When using Mozilla Firefox or Netscape to access the Network Camera and the video mode is set to **JPEG**, users will receive video comprised of continuous JPEG images. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape.

URL command -- **http://<ip address>:<http port>/<access name for stream 1 ~ 3>**
For example, when the Access name for **stream 2** is set to **video2.mjpg**:
1. Launch Mozilla **Firefox** or **Netscape**.
2. Type the above URL command in the address bar. Press **Enter**.
3. The JPEG images will be displayed in your web browser.



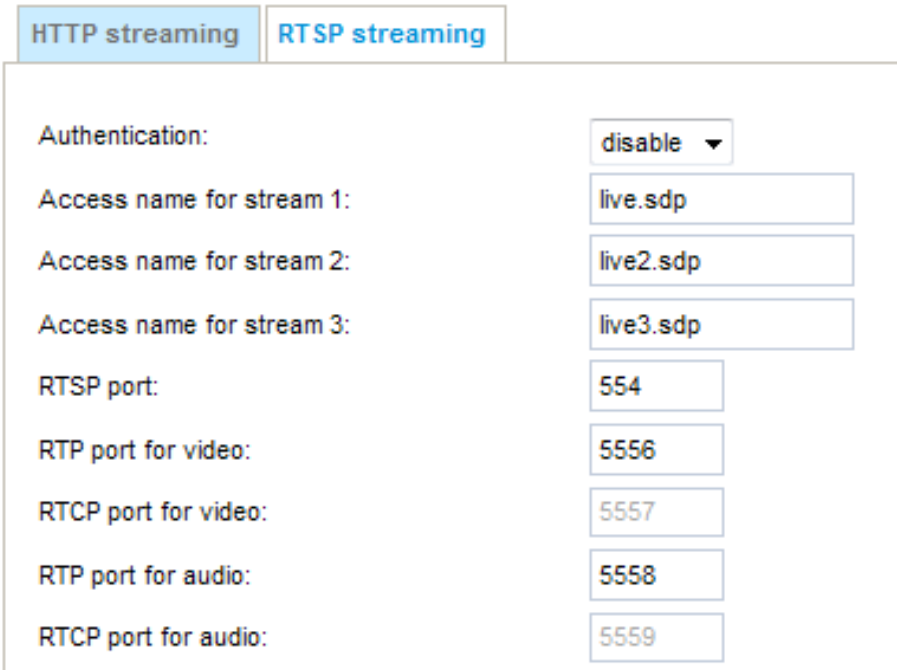

**IMPORTANT:**

► ***Microsoft® Internet Explorer*** *does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream 1 ~ 3> will fail to access the Network Camera.*

► *Users can only use URL commands to request the stream 5. For more information about URL commands, please refer to page 137.*

## RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for the Network Camera first; please refer to **Security > User account** on page 88 for details.



Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic, and digest.
If **basic** authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.
The availability of the RTSP streaming for the three authentication modes is listed in the following table:

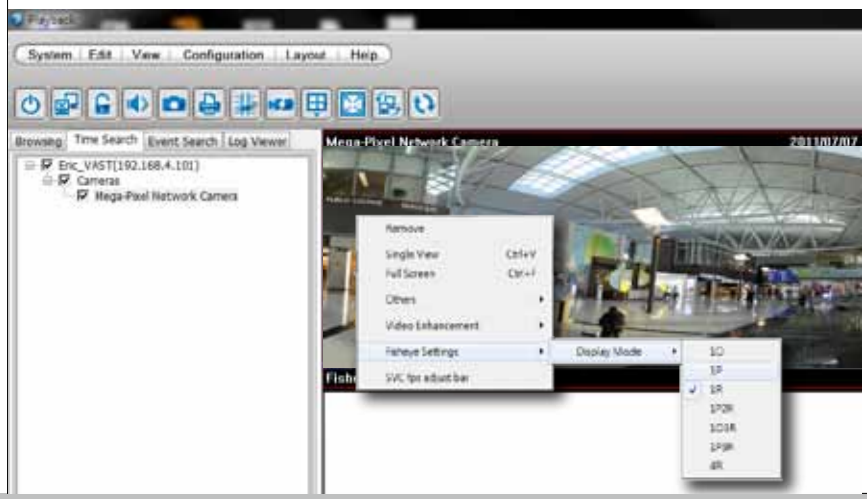
| | Quick Time player | Real Player |
|---|---|---|
| Disable | O | O |
| Basic | O | O |
| Digest | O | X |

Access name for stream 1 ~ 3: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.
If you want to use an RTSP player to access the Network Camera, you **HAVE TO** set the video mode to H.264 / MPEG-4 and use the following RTSP URL command to request transmission of the streaming data. rtsp://<ip address>:<rtsp port>/<access name for stream1 ~ 3>

For example, when the access name for stream 1 is set to live.sdp:
1. Launch an RTSP player.
2. Choose File > Open URL. A URL dialog box will pop up.
3. Type the above URL command in the address field.
4. The live video will be displayed in your player as shown below.


**NOTE:**

An original, circular view will be displayed using all RTSP players. For access to the Regional Views, you can install VIVOTEK's ST7501 or VAST software. You can right-click on a live view window to see the Display mode options.



RTSP port /RTP port for video, audio/ RTCP port for video, audio

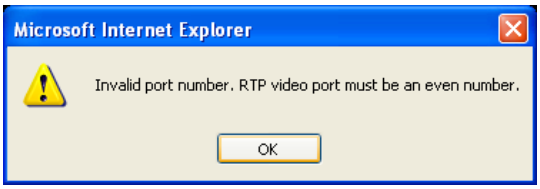
- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.

- The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.

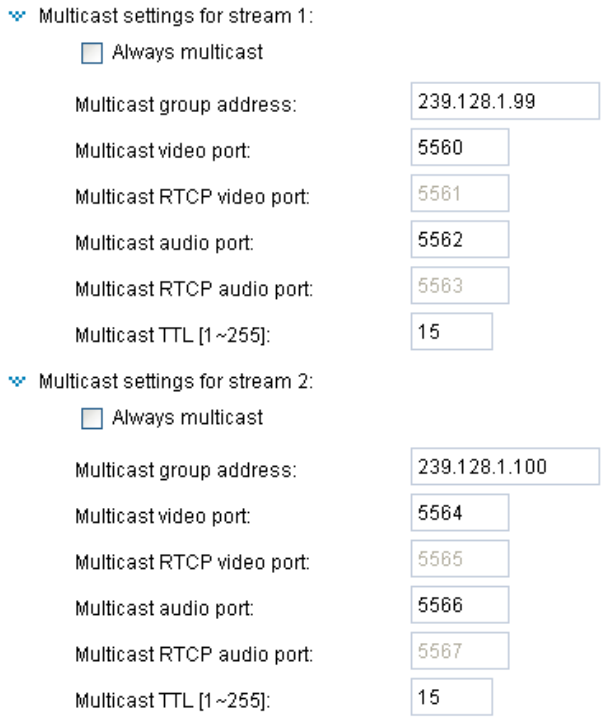
- The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always an odd number. When the RTP port changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message will be displayed:



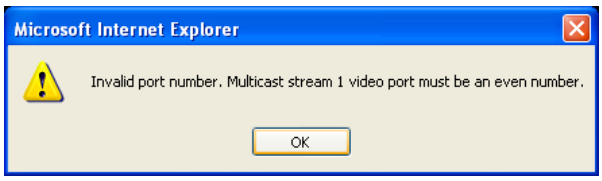
Multicast settings for stream 1 ~ 3: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for streams 1 ~ 3.




Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, enabling multicast can effectively save Internet bandwith.

The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus is always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will be displayed:




Multicast TTL [1~255]: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

# Network > QoS (Quality of Service) Advanced Mode

Quality of Service refers to a resource reservation control mechanism, which guarantees a certain quality to different services on the network. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. Quality can be defined as, for instance, a maintained level of bit rate, low latency, no packet dropping, etc.

The following are the main benefits of a QoS-aware network:
- The ability to prioritize traffic and guarantee a certain level of performance to the data flow.
- The ability to control the amount of bandwidth each application may use, and thus provide higher reliability and stability on the network.

## Requirements for QoS

To utilize QoS in a network environment, the following requirements must be met:
- All network switches and routers in the network must include support for QoS.
- The network video devices used in the network must be QoS-enabled.

## QoS models

### CoS (the VLAN 802.1p model)

IEEE802.1p defines a QoS model at OSI Layer 2 (Data Link Layer), which is called CoS, Class of Service. It adds a 3-bit value to the VLAN MAC header, which indicates the frame priority level from 0 (lowest) to 7 (highest). The priority is set up on the network switches, which then use different queuing disciplines to forward the packets.

Below is the setting column for CoS. Enter the **VLAN ID** of your switch (0~4095) and choose the priority for each application (0~7).


If you assign Video the highest priority level, your network switch will handle video packets first.

**NOTE:**

► *A VLAN-capable Switch (802.1p) is required. Web browsing may fail if the CoS setting is incorrect.*

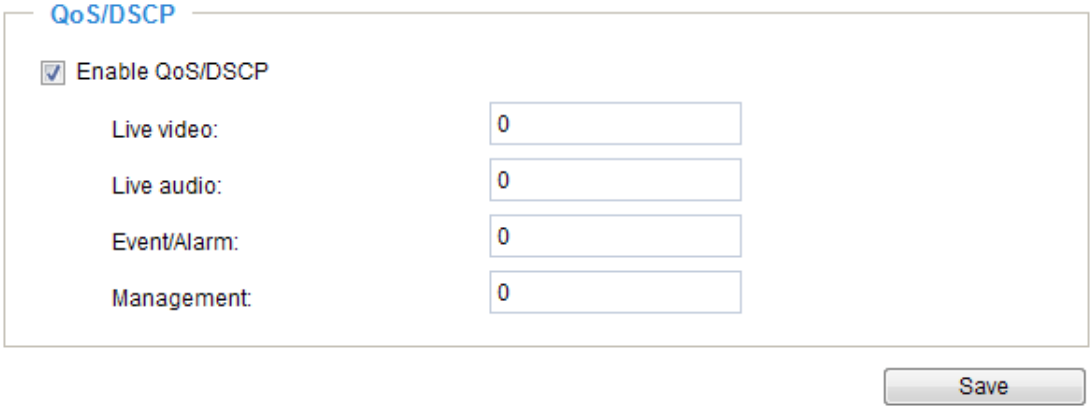
► *Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.*

► *Although CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees since it is based on L2 protocol.*

## QoS/DSCP (the DiffServ model)

DSCP-ECN defines QoS at Layer 3 (Network Layer). The Differentiated Services (DiffServ) model is based on packet marking and router queuing disciplines. The marking is done by adding a field to the IP header, called the DSCP (Differentiated Services Codepoint). This is a 6-bit field that provides 64 different class IDs. It gives an indication of how a given packet is to be forwarded, known as the Per Hop Behavior (PHB). The PHB describes a particular service level in terms of bandwidth, queueing theory, and dropping (discarding the packet) decisions. Routers at each network node classify packets according to their DSCP value and give them a particular forwarding treatment; for example, how much bandwidth to reserve for it.

Below are the setting options of DSCP (DiffServ Codepoint). Specify the DSCP value for each application (0~63).

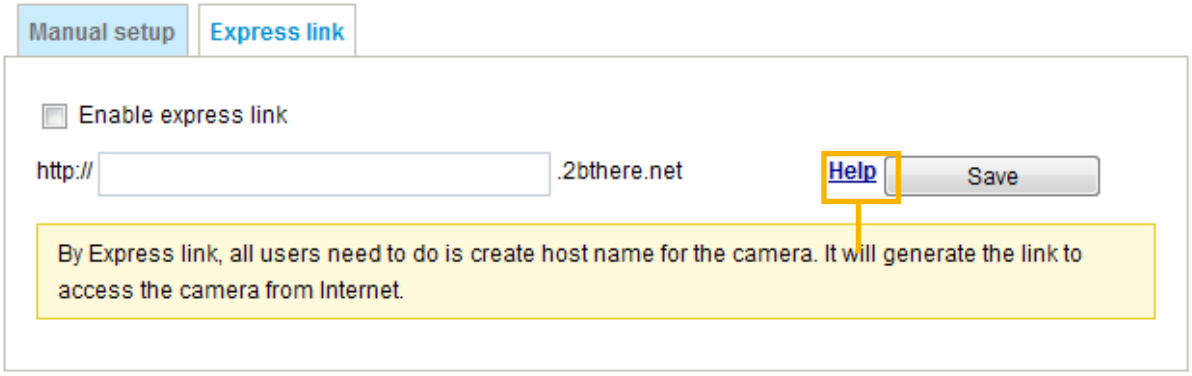


# Network > DDNS

This section explains how to configure the dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

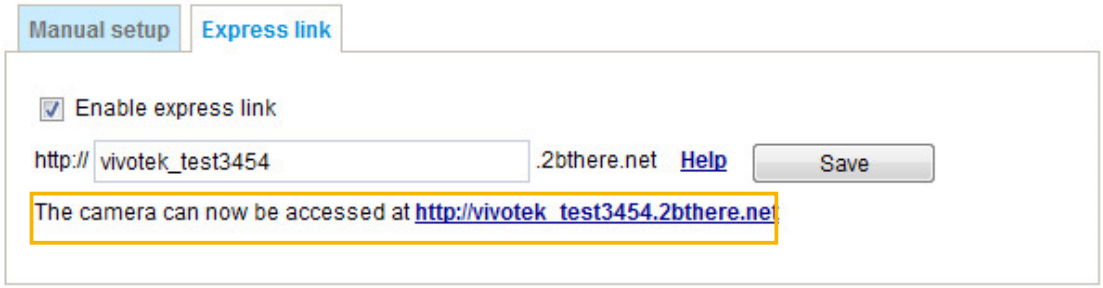
## Express link

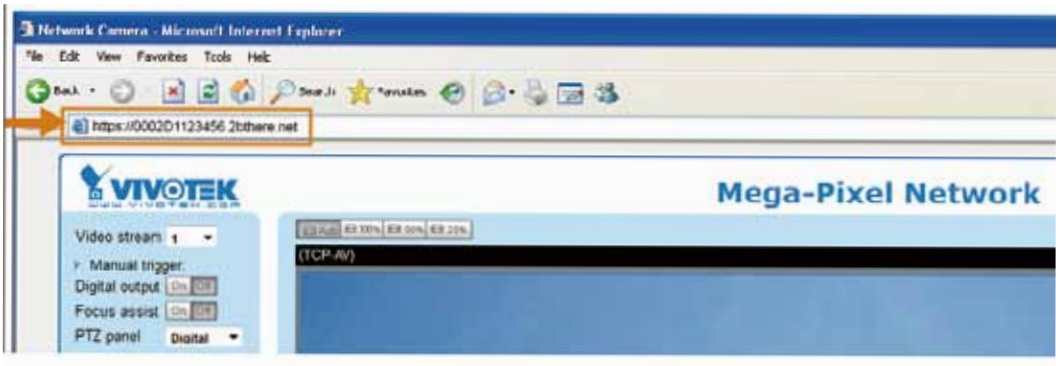
Express Link is a free service provided by VIVOTEK server, which allows users to register a domain name for a network device. One URL can only be mapped to one MAC address. This service will check out if the host name is valid and automatically open a port on your router. Unlike DDNS, which requires a user to manually check out details about UPnP port forwarding, the Express Link is more convenient and easy to set up.




Please follow the steps below to enable Express Link:

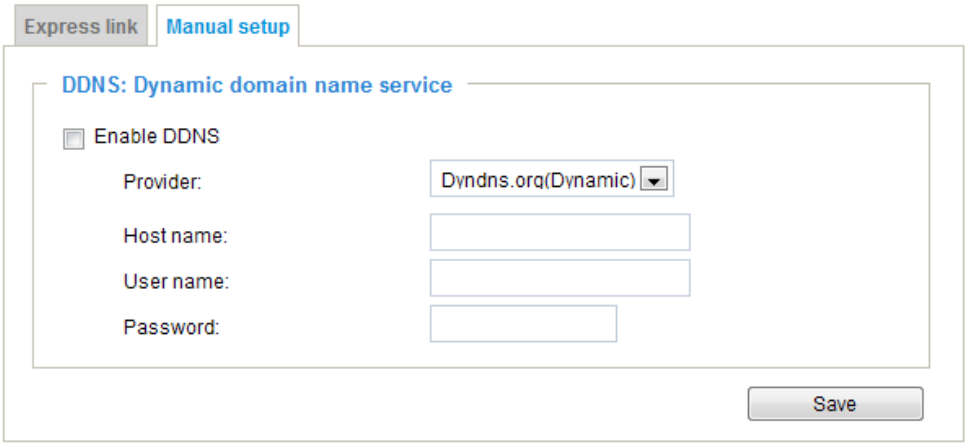
1. Make sure that your router supports UPnP port forwarding and it is activated, or you may see the following warning message: Express link is not supported under current network environment.
2. Check **Enable express link**.
3. Enter a host name for the network device and click **Save**. If the host name has been used by another device, a warning message will show up. If the host name is valid, it will show a message as shown below.



## Manual setup

### DDNS: Dynamic domain name service

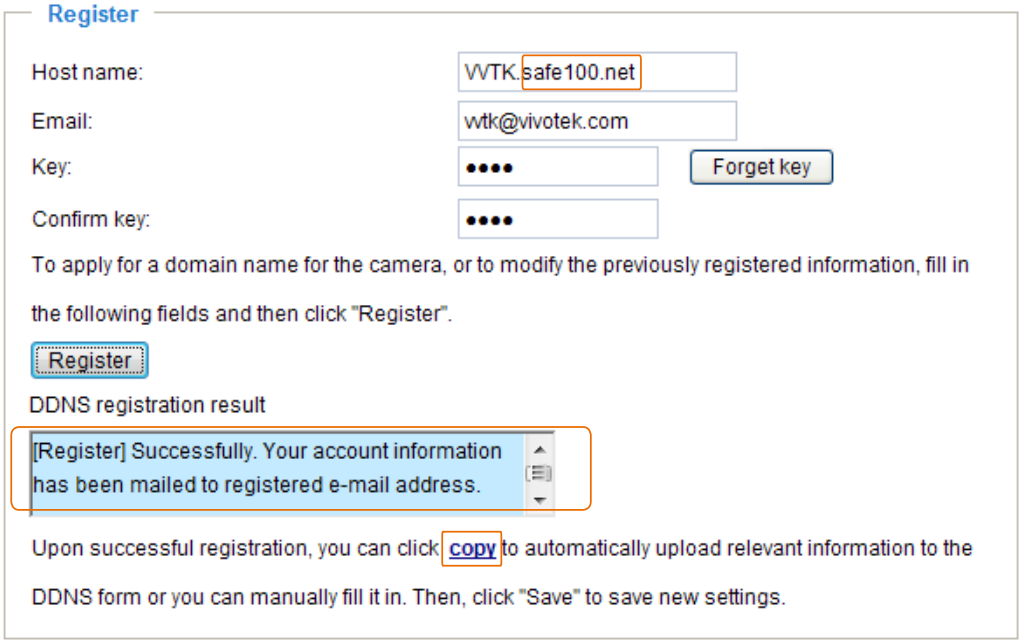



Enable DDNS: Select this option to enable the DDNS setting.

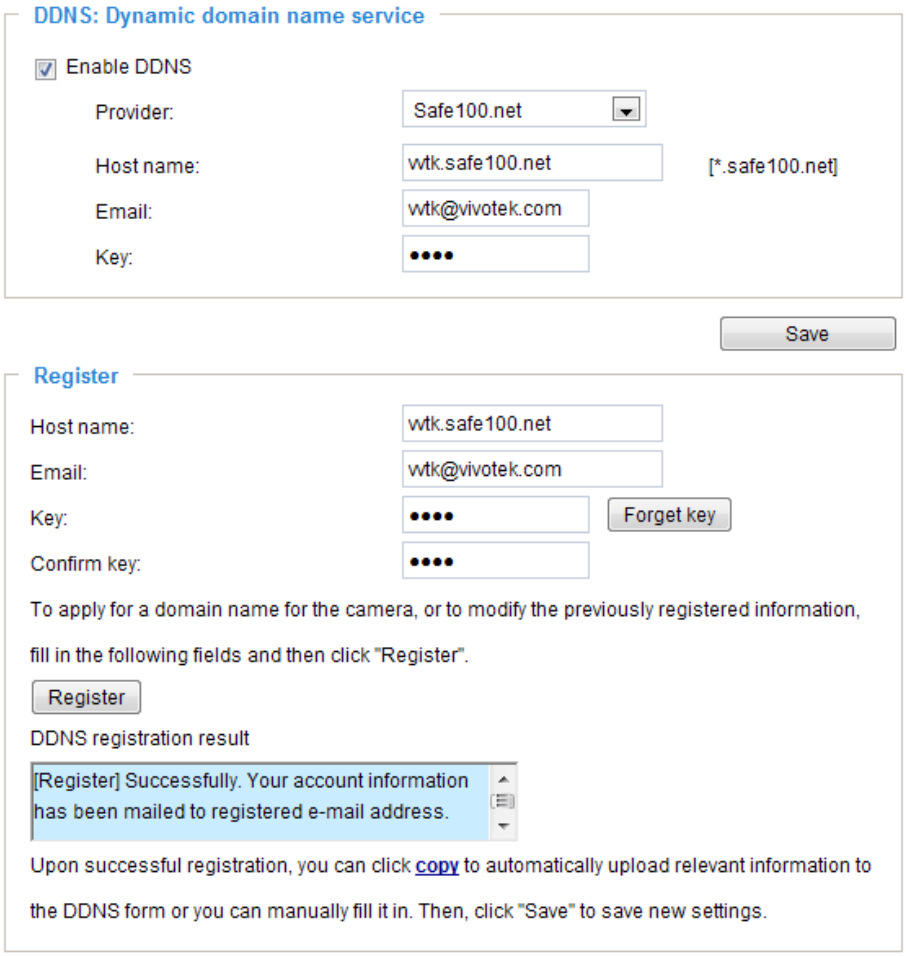
Provider: Select a DDNS provider from the provider drop-down list.
VIVOTEK offers **Safe100.net**, a free dynamic domain name service, to VIVOTEK customers. It is recommended that you register **Safe100.net** to access VIVOTEK's Network Cameras from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO.com, DHS.org, CustomSafe100, dyn-interfree.it.
Note that before utilizing this function, please apply for a dynamic domain account first.

■ Safe100.net

1. In the DDNS column, select **Safe100.net** from the drop-down list. Click **I accept** after reviewing the terms of the Service Agreement.
2. In the Register column, fill in the Host name (xxxx.safe100.net), Email, Key, and Confirm Key, and click **Register**. After a host name has been successfully created, a success message will be displayed in the DDNS Registration Result column.




3. Click **Copy** and all the registered information will automatically be uploaded to the corresponding fields in the DDNS column at the top of the page as seen in the following screen.




4. Select Enable DDNS and click **Save** to enable the setting.

■ CustomSafe100

VIVOTEK offers documents to establish a CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

1. In the DDNS column, select CustomSafe100 from the drop-down list.
2. In the Register column, fill in the Host name, Email, Key, and Confirm Key; then click **Register**. After a host name has been successfully created, you will see a success message in the DDNS Registration Result column.
3. Click **Copy** and all for the registered information will be uploaded to the corresponding fields in the DDNS column.
4. Select Enable DDNS and click **Save** to enable the setting.

Forget key: Click this button if you have forgotten the key to Safe100.net or CustomSafe100. Your account information will be sent to your email address.

Refer to the following links to apply for a dynamic domain account when selecting other DDNS providers:

■ Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/
■ dyn-interfree.it: visit http://dyn-interfree.it/

# Network > SNMP (Simple Network Management Protocol)

Advanced Mode

This section explains how to use the SNMP on the network camera. The Simple Network Management Protocol is an application layer protocol that facilitates the exchange of management information between network devices. It helps network administrators to remotely manage network devices and find, solve network problems with ease.

■ The SNMP consists of the following three key components:
1. Manager: Network-management station (NMS), a server which executes applications that monitor and control managed devices.
2. Agent: A network-management software module on a managed device which transfers the status of managed devices to the NMS.
3. Managed device: A network node on a managed network. For example: routers, switches, bridges, hubs, computer hosts, printers, IP telephones, network cameras, web server, and database.

Before configuring SNMP settings on the this page, please enable your NMS first.

## SNMP Configuration

Enable SNMPv1, SNMPv2c

Select this option and enter the names of Read/Write community and Read Only community according to your NMS settings.


Enable SNMPv3

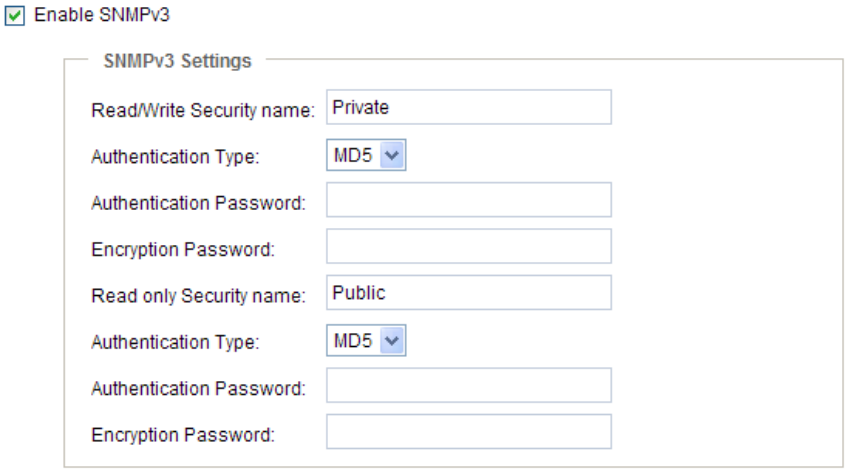
This option contains cryptographic security, a higher security level, which allows you to set the Authentication password and the Encryption password.

■ Security name: According to your NMS settings, choose Read/Write or Read Only and enter the community name.

■ Authentication type: Select MD5 or SHA as the authentication method.

■ Authentication password: Enter the password for authentication (at least 8 characters).

■ Encryption password: Enter a password for encryption (at least 8 characters).



# Security > User Account

This section explains how to enable password protection and create multiple accounts.

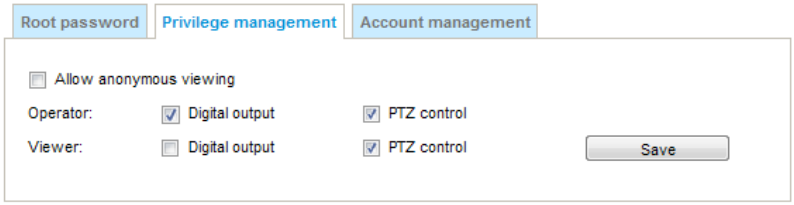
## Root Password


The administrator account name is “root”, which is permanent and can not be deleted. If you want to add more accounts in the Manage User column, please apply the password for the “root” account first.

1. Type the password identically in both text boxes, then click **Save** to enable password protection.
2. A window will prompt for authentication; type the correct user’s name and password in their respective fields to access the Network Camera.

## Privilege management

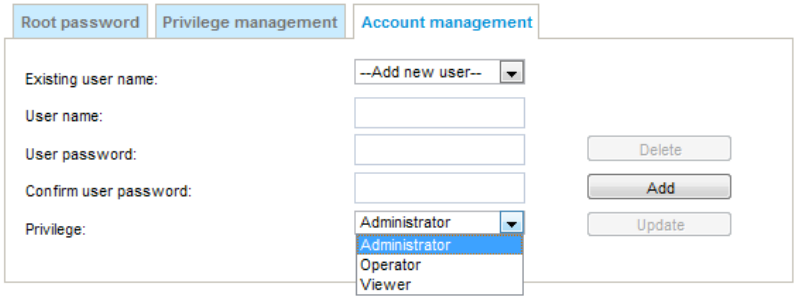
Advanced Mode




Digital Output & PTZ control: You can modify the management privilege as operators or viewers. Select or de-select the checkboxes, and then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page. (Please refer to Configuration on page 41).

Allow anonymous viewing: If you select this item, any client can access the live stream without entering a User ID and Password.

## Account management




Administrators can create up to 20 user accounts.

1. Input the new user’s name and password.
2. Select the privilege level for the new user account. Click **Add** to enable the setting.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Though operators cannot access the Configuration page, they can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 136. Viewers access only the main page for live viewing.

Here you also can change a user’s access rights or delete user accounts.

1. Select an existing account to modify.
2. Make necessary changes and click **Update** or **Delete** to enable the setting.

# Security > HTTPS (Hypertext Transfer Protocol over SSL)

Advanced Mode

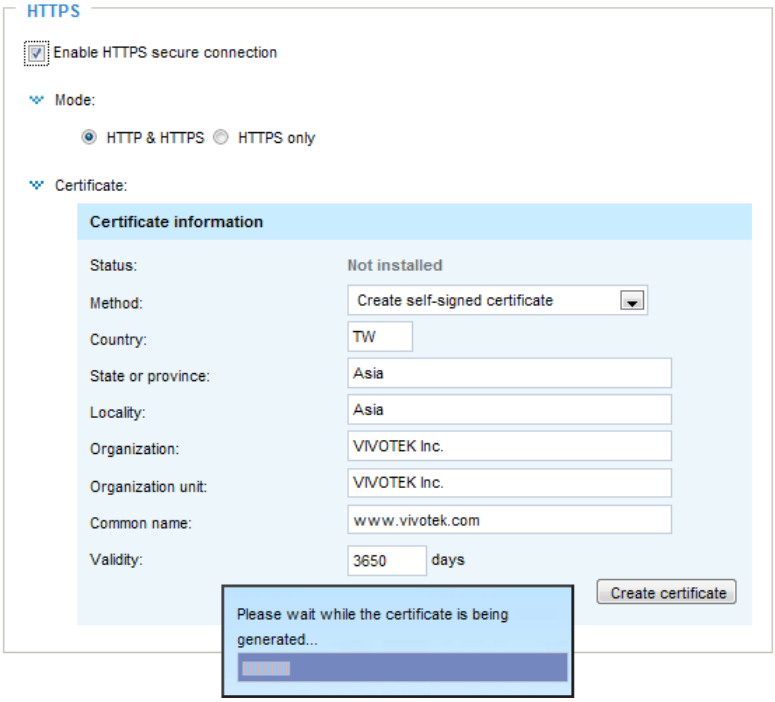
This section explains how to enable authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher security level.

## Create and Install Certificate Method

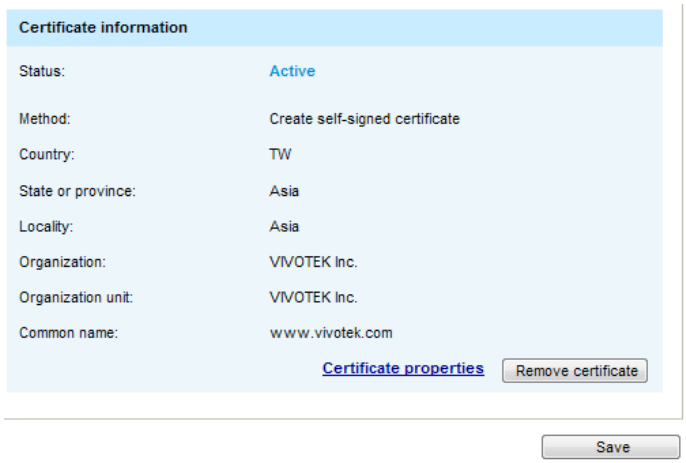
Before using HTTPS for communication with the Network Camera, a **Certificate** must be created first. There are three ways to create and install a certificate:

### Create self-signed certificate

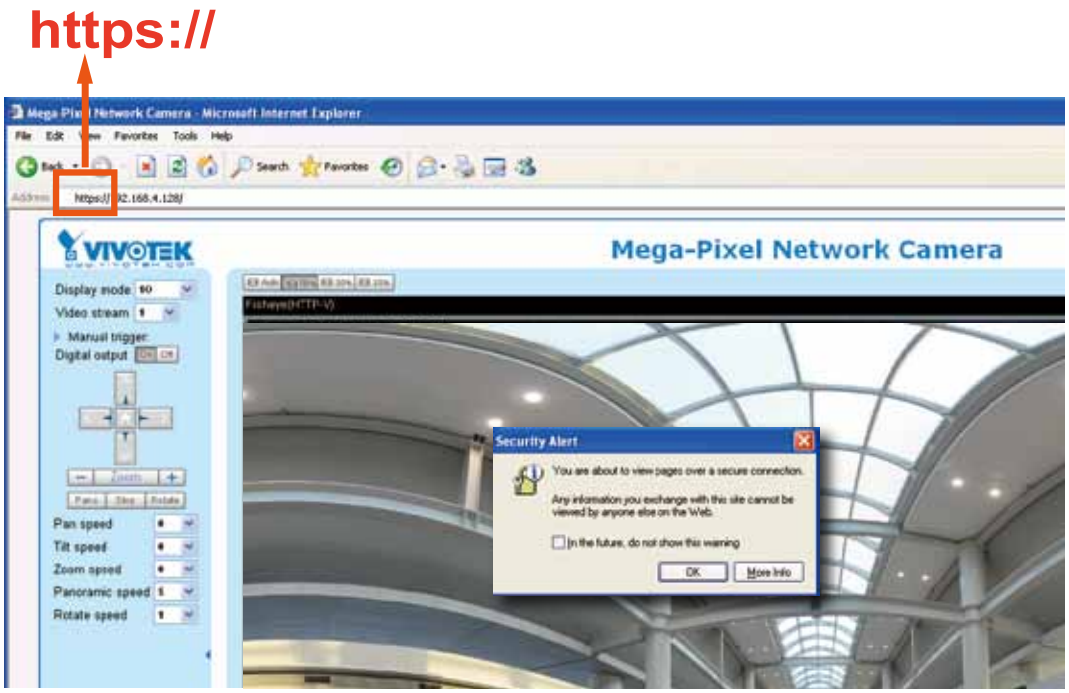
1. Select the first option.
2. Check **Enable HTTPS secure connection**, then select a connection option: “HTTP & HTTPS” or “HTTPS only”.
3. Click **Create certificate** to generate a certificate.



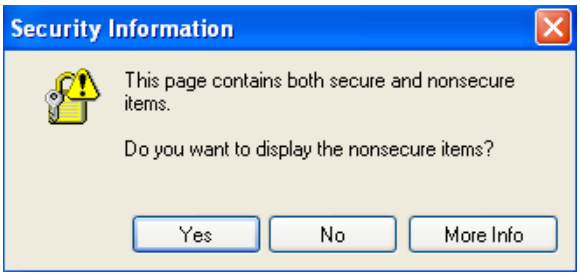

4. The Certificate Information will automatically be displayed in the lower screen as shown below. You can click **Certificate properties** to view detailed information about the certificate.



5. Click **Save** to preserve your configuration, and your current session with the camera will change to the encrypted connection.
6. If your web session does not automatically change to an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.



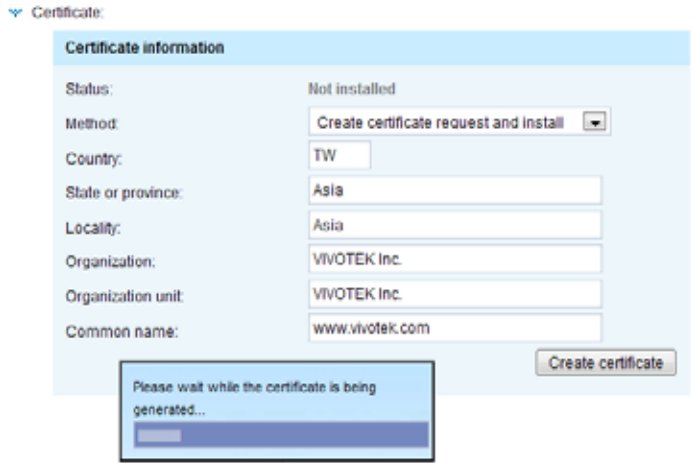




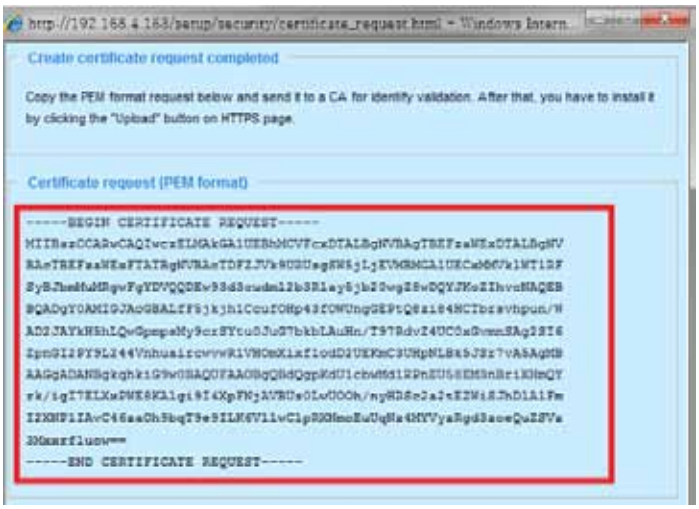
## Create certificate request and install

1. Select the option from the **Method** pull-down menu.
2. Click **Create certificate** to proceed.

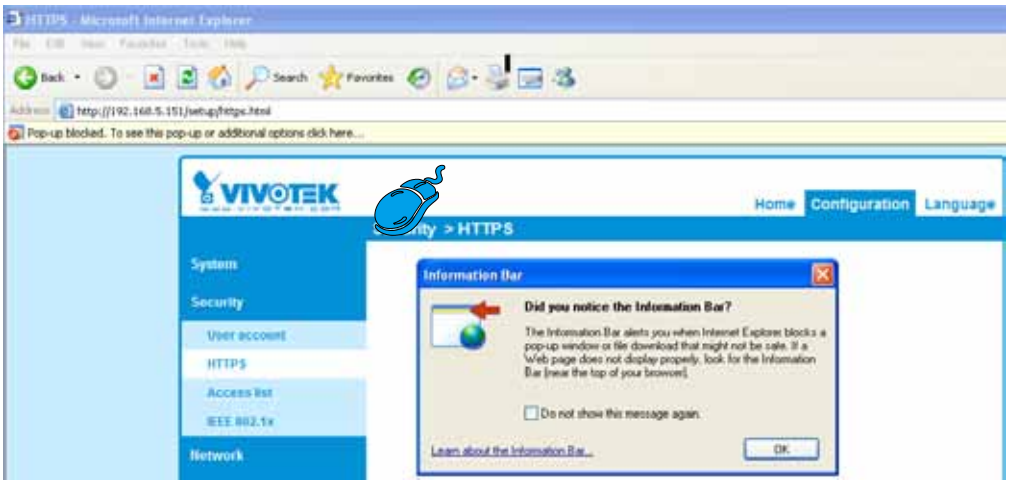
3. The following information will show up in a pop-up window after clicking **Create**. Then click **Save** to generate the certificate request.



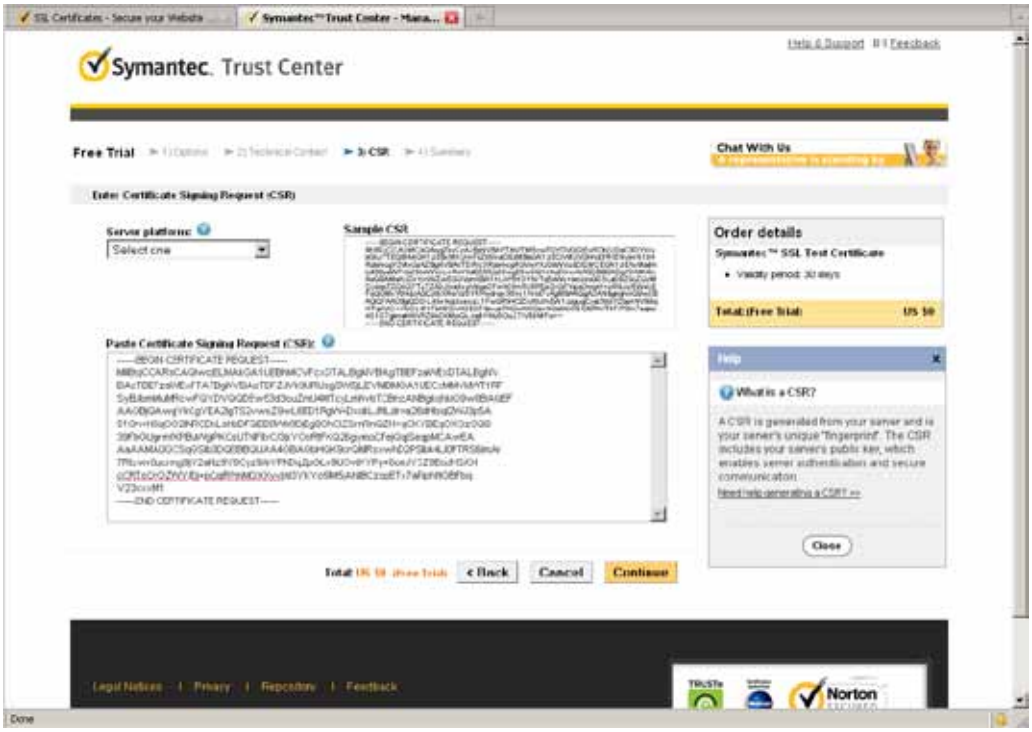

4. The Certificate request window will prompt.




If you see the following Information bar, click **OK** and click on the Information bar at the top of the page to allow pop-ups.

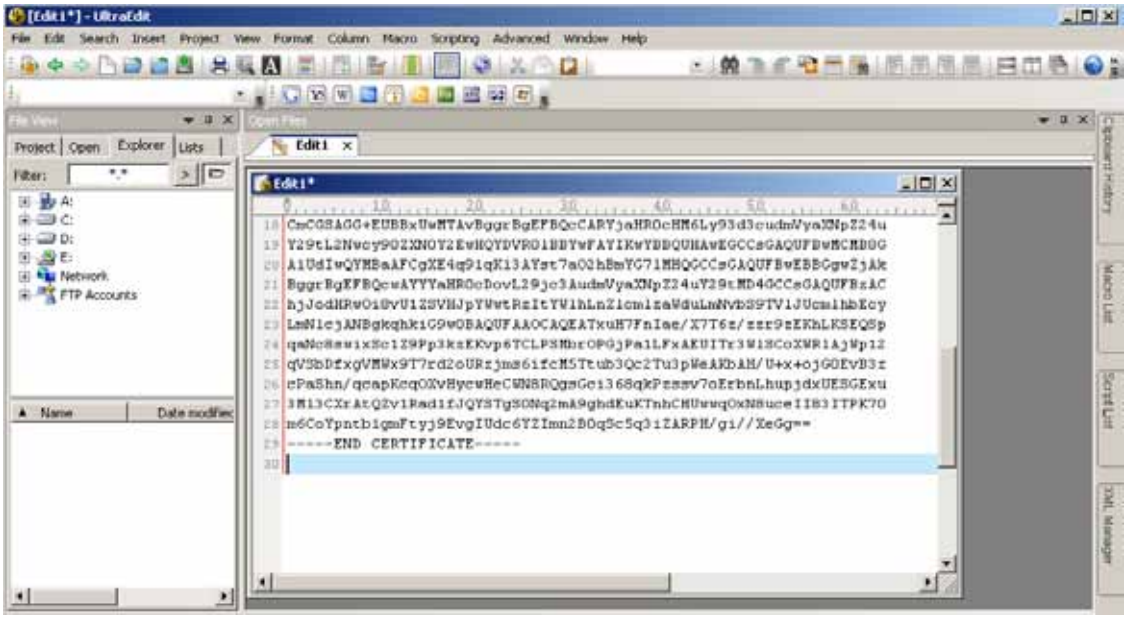


5. Look for a trusted certificate authority, such as Symantec's VeriSign Authentication Services, that issues digital certificates. Sign in and purchase the SSL certification service. Copy the certificate request from your request prompt and paste it in the CA's signing request window. Proceed with the rest of the process as CA's instructions on their webpage.

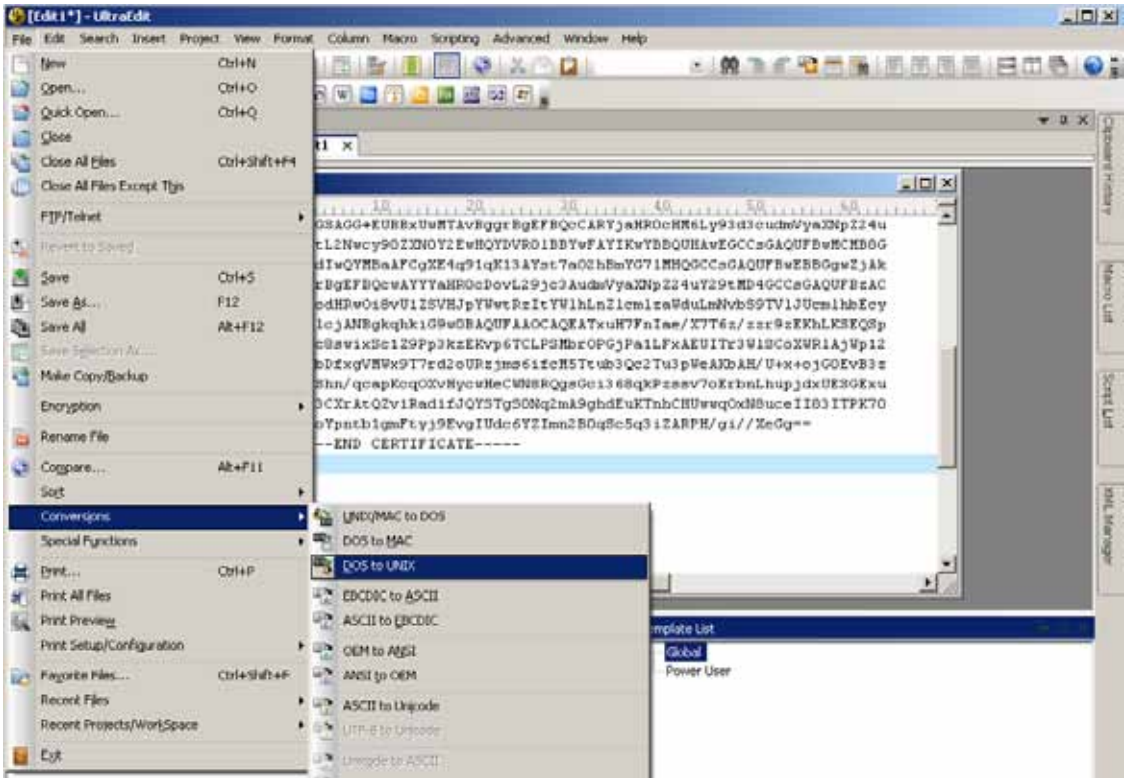



6. Once completed, your SSL certificate should be delivered to you via an email or other means. Copy the contents of the certificate in the email and paste it in a text/HTML/hex editor/converter, such as IDM Computer Solutions' UltraEdit.

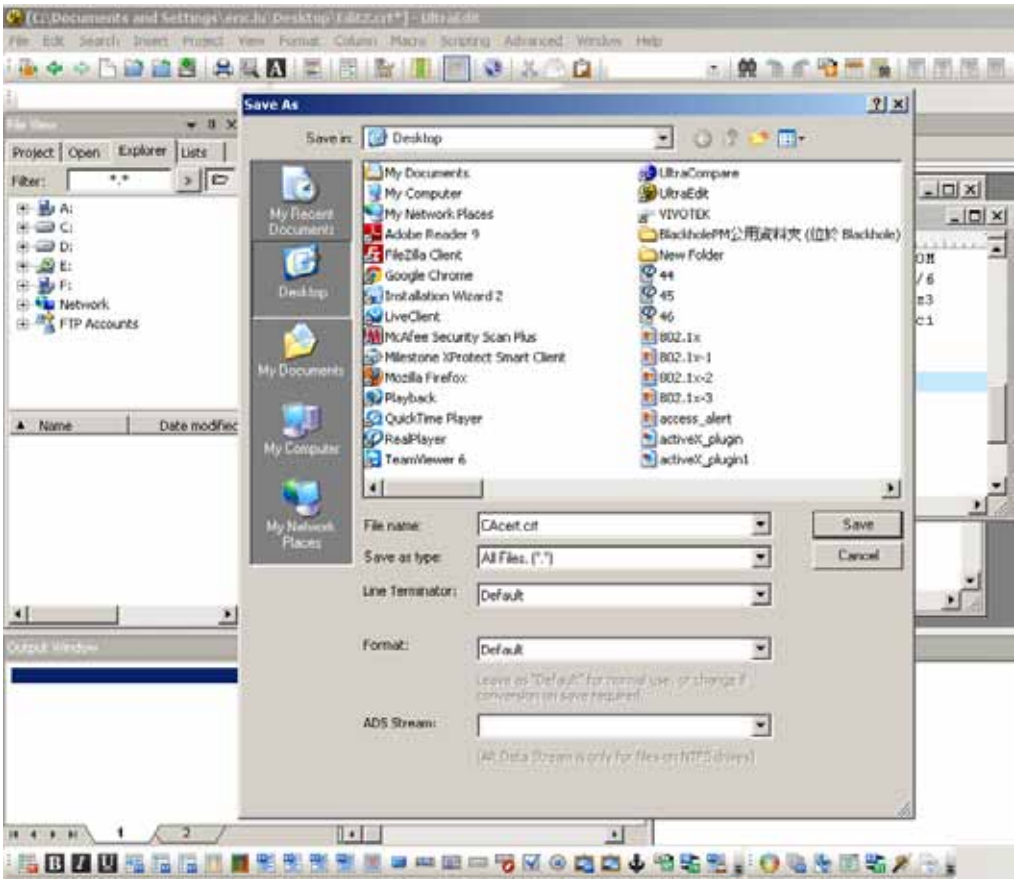
7. Open a new edit, paste the certificate contents, and press ENTER at the end of the contents to add an empty line.




8. Convert file format from DOS to UNIX. Open **File** menu > **Conversions** > **DOS to Unix**.

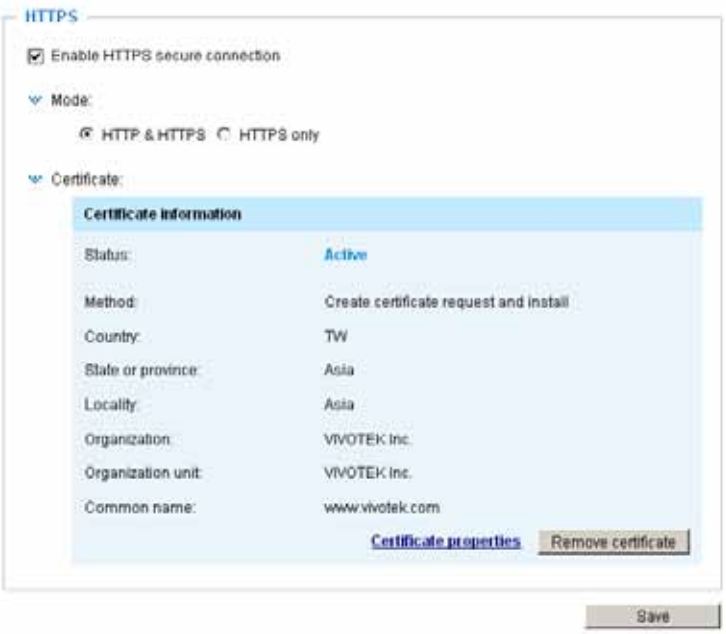


9. Save the edit using the ".crt" extension, using a file name like "CAcert.crt."

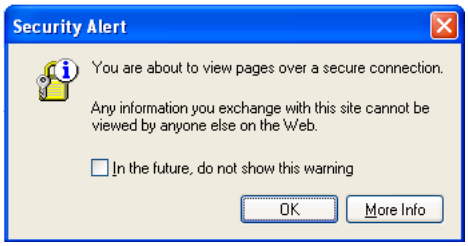


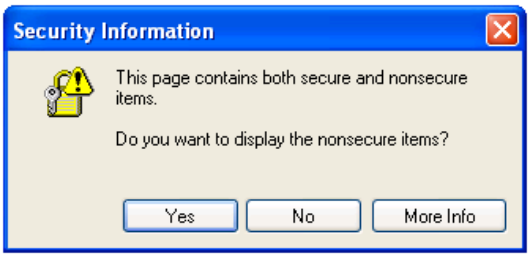

10. Return to the original firmware session, use the **Browse** button to locate the crt certificate file, and click **Upload** to enable the certification.

11. When the certifice file is successfully loaded, its status will be stated as **Active**. Note that a certificate must have been created and installed before you can click on the "**Save**" button for the configuration to take effect.




12. To begin an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.



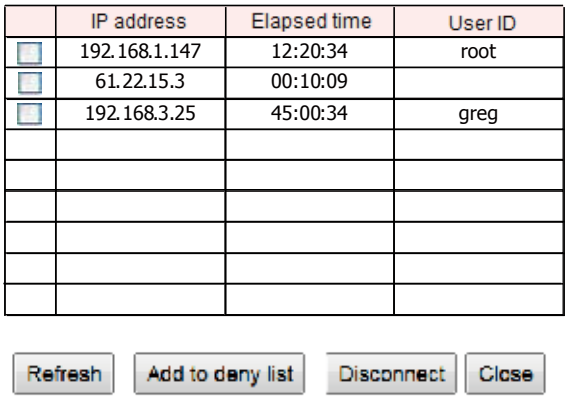

# Security > Access List Advanced Mode

This section explains how to control access permission by verifying the client PC's IP address.

## General Settings


Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream 1 and stream 2). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (IE Explore or Quick Time Player).

Connection management: Click this button to display the connection status window showing a list of the current connections. For example:




■ IP address: Current connections to the Network Camera.

■ Elapsed time: How much time the client has been at the webpage.

■ User ID: If the administrator has set a password for the webpage, the clients have to enter a user name and password to access the live video. The user name will be displayed in the User ID column. If the administrator allows clients to link to the webpage without a user name and password, the User ID column will be empty.

There are some situations which allow clients access to the live video without a user name and password:

1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security > User account on page 88.
2. The administrator has set up a root password, but set **RTSP Authentication** to "disable". For more information about **RTSP Authentication**, please refer to RTSP Streaming on page 78.
3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing,** please refer to page 88.

■ Refresh: Click this button to refresh all current connections.

■ Add to deny list: You can select entries from the Connection Status list and add them to the Deny List to deny access. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player). If you want to enable the denied list, please check **Enable access list filtering** and click **Save** in the first column.

- Disconnect: If you want to break off the current connections, please select them and click this button. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explorer or Quick Time Player).

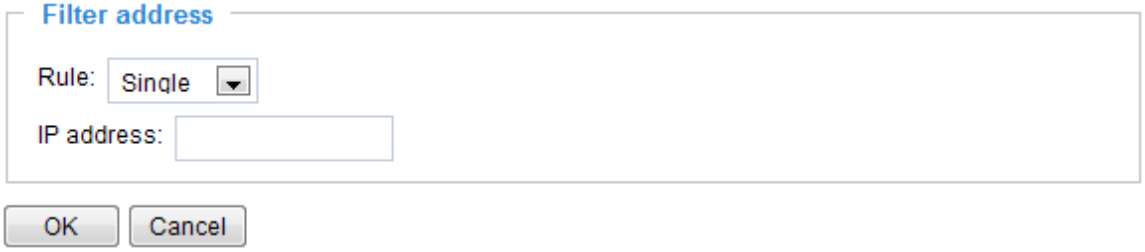
Enable access list filtering: Check this item and click **Save** if you want to enable the access list filtering function.

## Filter

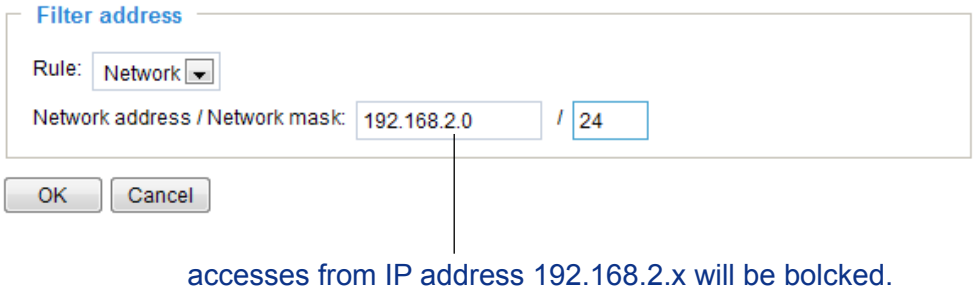
Filter type: Select **Allow** or **Deny** as the filter type. If you choose **Allow Type**, only those clients whose IP addresses are on the Access List below can access the Network Camera, and the others cannot access. On the contrary, if you choose **Deny Type**, those clients whose IP addresses are on the Access List below will not be allowed to access the Network Camera, and the others can access.

Then you can **Add** a rule to the following Access List. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to Network > Enable IPv6 on page 73 for detailed information.


There are three types of rules:
Single: This rule allows the user to add an IP address to the Allowed/Denied list.
For example:

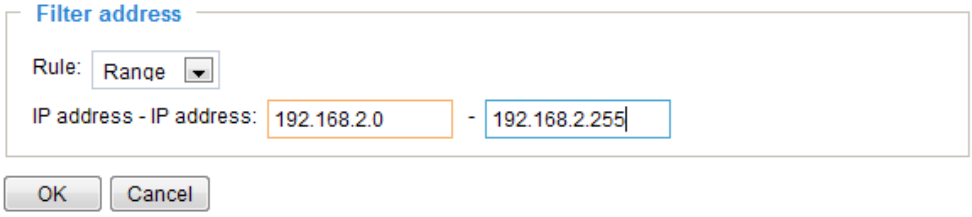


Network: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List. The routing prefix is written in CIDR notation. For example:



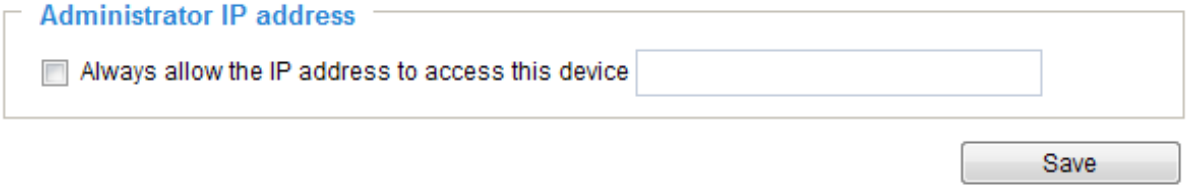

If IPv6 filter is preferred, you will be prompted by the following window. Enter the IPv6 address and the two-digit prefix length to specify the range of IP addresses in your configuration.


Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List.
Note: This rule is only applied to IPv4.
For example:




## Administrator IP address

Always allow the IP address to access this device: You can check this item and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.



# Security > IEEE 802.1x Advanced Mode

Enable this function if your network environment uses IEEE 802.1x, which is a port-based network access control. The network devices, intermediary switch/access point/hub, and RADIUS server must support and enable 802.1x settings.

The 802.1x standard is designed to enhance the security of local area networks, which provides authentication to network devices (clients) attached to a network port (wired or wireless). If all certificates between client and server are verified, a point-to-point connection will be enabled; if authentication fails, access on that port will be prohibited. 802.1x utilizes an existing protocol, the Extensible Authentication Protocol (EAP), to facilitate communication.

■ The components of a protected network with 802.1x authentication:

Supplicant
(Network Camera)

Authenticator
(Network Switch)

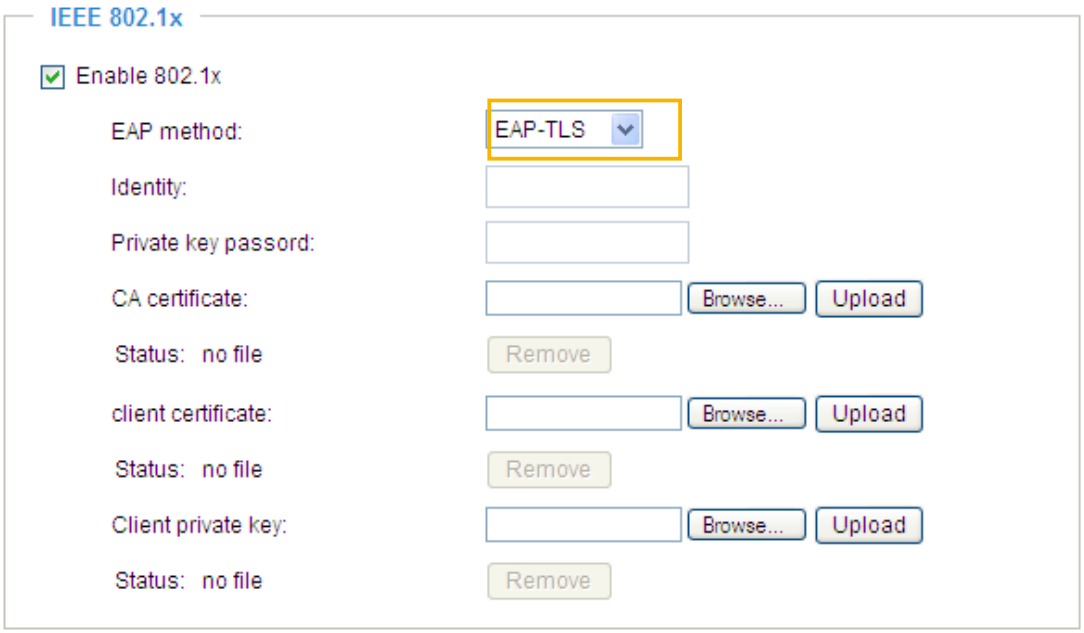
Authentication Server
(RADIUS Server)

1. Supplicant: A client end user (camera), which requests authentication.
2. Authenticator (an access point or a switch): A “go between” which restricts unauthorized end users from communicating with the authentication server.
3. Authentication server (usually a RADIUS server): Checks the client certificate and decides whether to accept the end user’s access request.

■ VIVOTEK Network Cameras support two types of EAP methods to perform authentication: **EAP-PEAP** and **EAP-TLS**.

Please follow the steps below to enable 802.1x settings:

1. Before connecting the Network Camera to the protected network with 802.1x, please apply a digital certificate from a Certificate Authority (i.e., MIS of your company) which can be validated by a RADIUS server.
2. Connect the Network Camera to a PC or notebook outside of the protected LAN. Open the configuration page of the Network Camera as shown below. Select **EAP-PEAP** or **EAP-TLS** as the EAP method. In the following blanks, enter your ID and password issued by the CA, then upload related certificate(s).

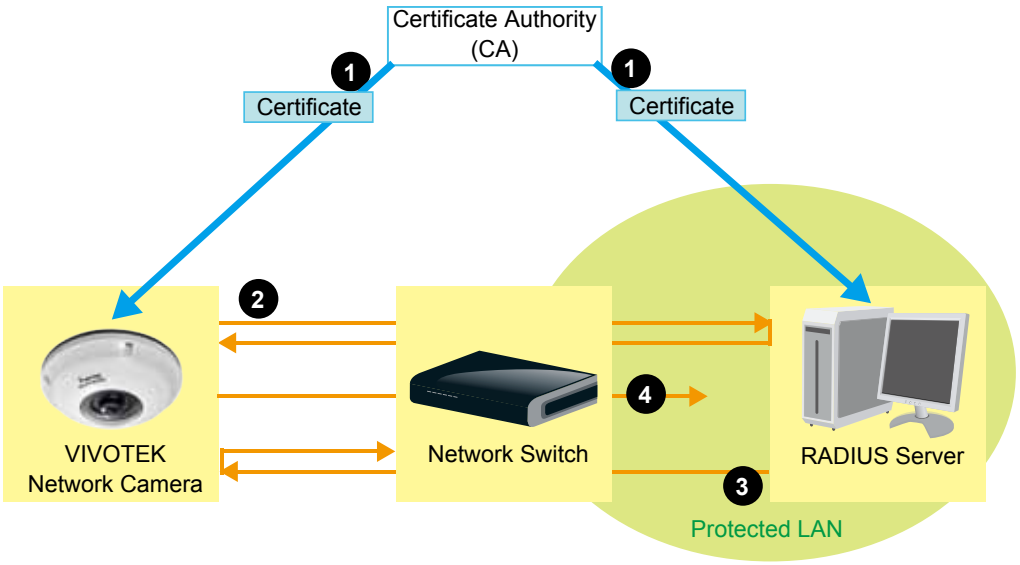



3. When all settings are complete, move the Network Camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.

**NOTE:**

► *The authentication process for 802.1x:*

1. *The Certificate Authority (CA) provides the required signed certificates to the Network Camera (the supplicant) and the RADIUS Server (the authentication server).*
2. *A Network Camera requests access to the protected LAN using 802.1X via a switch (the authenticator). The client offers its identity and client certificate, which is then forwarded by the switch to the RADIUS Server, which uses an algorithm to authenticate the Network Camera and returns an acceptance or rejection back to the switch.*
3. *The switch also forwards the RADIUS Server's certificate to the Network Camera.*
4. *Assuming all certificates are validated, the switch then changes the Network Camera's state to authorized and is allowed access to the protected network via a pre-configured port.*

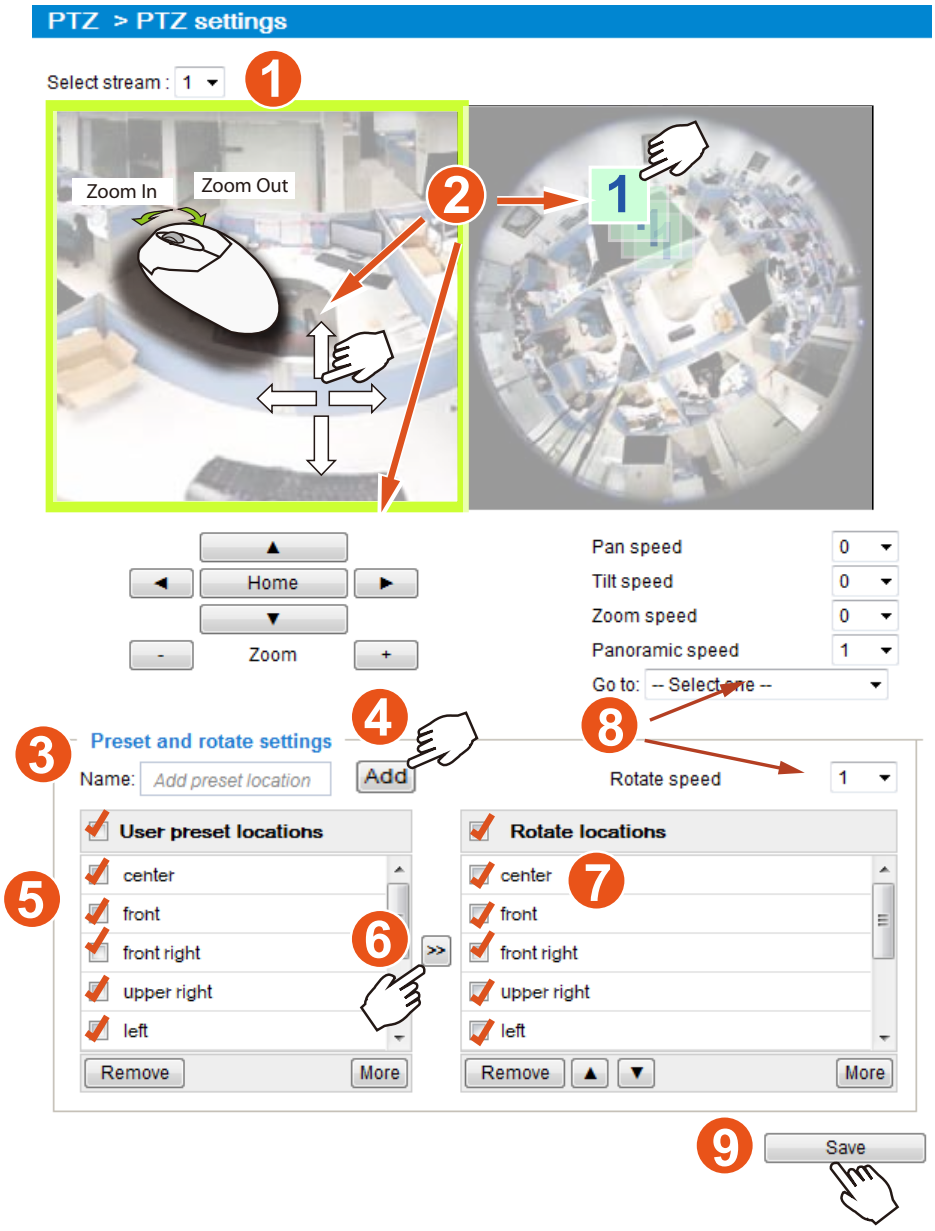


# PTZ > PTZ settings Advanced Mode

This section explains how to control the Network Camera's Pan/Tilt/Zoom operation.

The PTZ function allows users to quickly move the focus to a target area for close-up viewing without physically zooming the camera.

## Digital PTZ Operation (E-PTZ Operation)




Preset positions and rotation settings

In the PTZ settings page, you can create preset positions in the hemisphere covered by the fisheye lens. A total of 20 preset positions can be configured.

Please follow the steps below to configure preset positions and arrange them in a rotational tour through different positions.

1. First select a video stream on which the PTZ settings will take place.

2. Adjust the shooting area to the desired position using the PTZ keypad, the FOV indicators, or mouse clicks on the live screen. To begin the mouse control, click on the two interactive windows. If you click on the Original view window, an **FOV indicator** will appear. You can click and hold down the left mouse button to drag the FOV indicator to a desired position. The rest of mouse control methods are identical to those for the Regional windows.

   Due to the highly-sensitive mouse control, the PTZ control buttons can help fine-tune to an optimal location.

   Please note that your PTZ preset settings will only take effect on Regional windows, and not on the Panoramic views.

3. After you selected an area of interest, enter a name for the new position, which can contain up to forty characters.

4. Click **Add** to enable the settings. The preset positions will be listed on the **User preset locations**. (To add more positions you wish, please repeat steps 1~3.)

5. Select the preset positions by their checkboxes.

6. Click on the move button (>>)  to move positions to the Rotate locations window.

7. You may select some or all of the imported positions as the stop points during the tour.

8. Select other speed options using their specific pull-down menus.

9. Select a preferred **Rotate speed** for consecutively displaying views of multiple positions. The Rotate speeds and the dwell time of each position on a Regional view window are shown below:

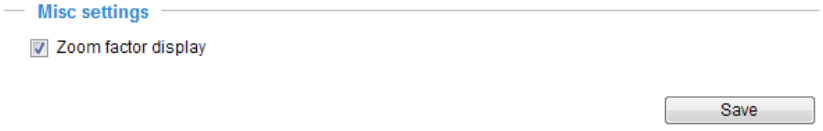
| Rotate speed | Dwell time in sec. |
|---|---|
| 1 | 6 |
| 2 | 3 |
| 3 | 2 |
| 4 | 1.5 |
| 5 | 1.2 |

9. Click on the **Save** button to preserve your configuration.

   To remove a preset position from the list, select it and click **Remove**. You can re-arrange the order of the position hop on the list using the  buttons.

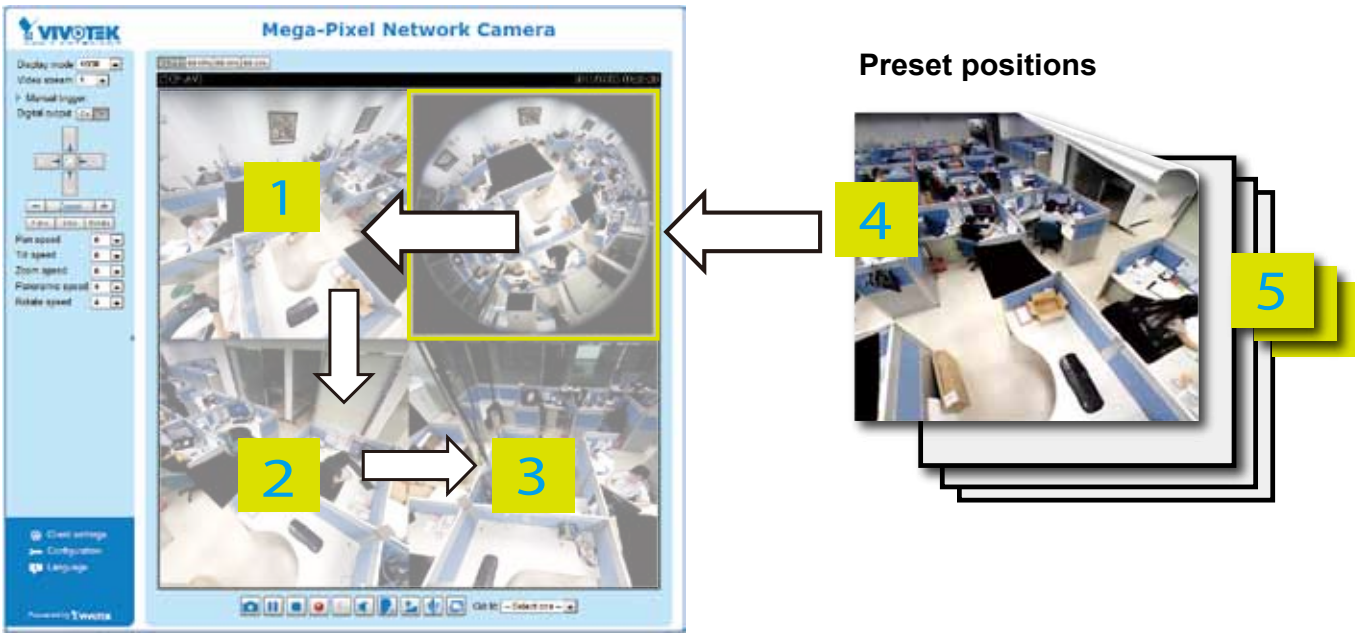
Misc settings

Use this checkbox to display or hide the zoom ratio indicator on the screen. You can use your mousewheel to zoom in or zoom out on a live view window.



Home page in Regional Display Mode

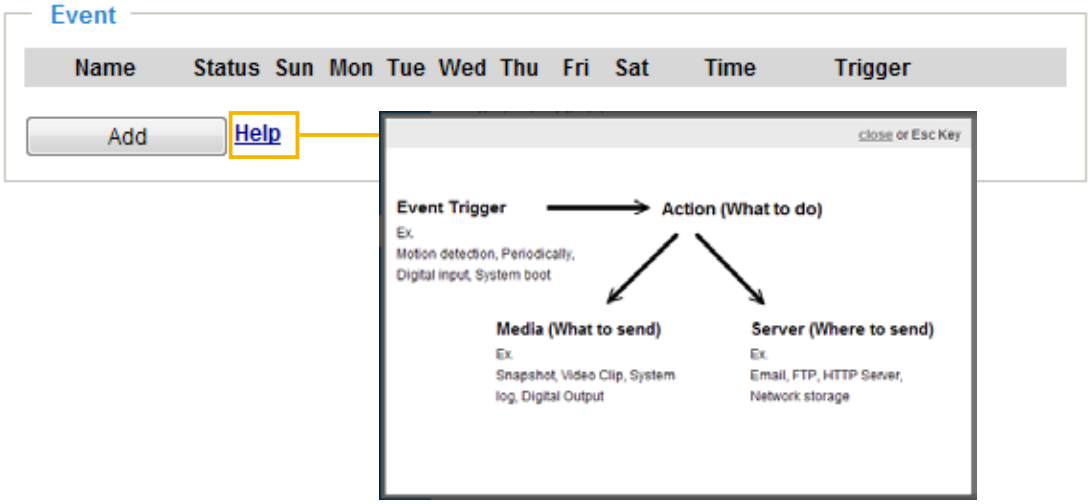
Shown below is the display order of preset positions when you click on the **Rotate** button on the main page.




- The preset positions will also be displayed on the home page. Select one from the **Go to** drop-down list, and the preset position will display on one of the Regional view windows.
- If you have set up different preset positions for different streams, you can select one of the video streams to display its distinctive positions.
- If there are multiple preset positions, these positions will take turn filling in your live view windows.

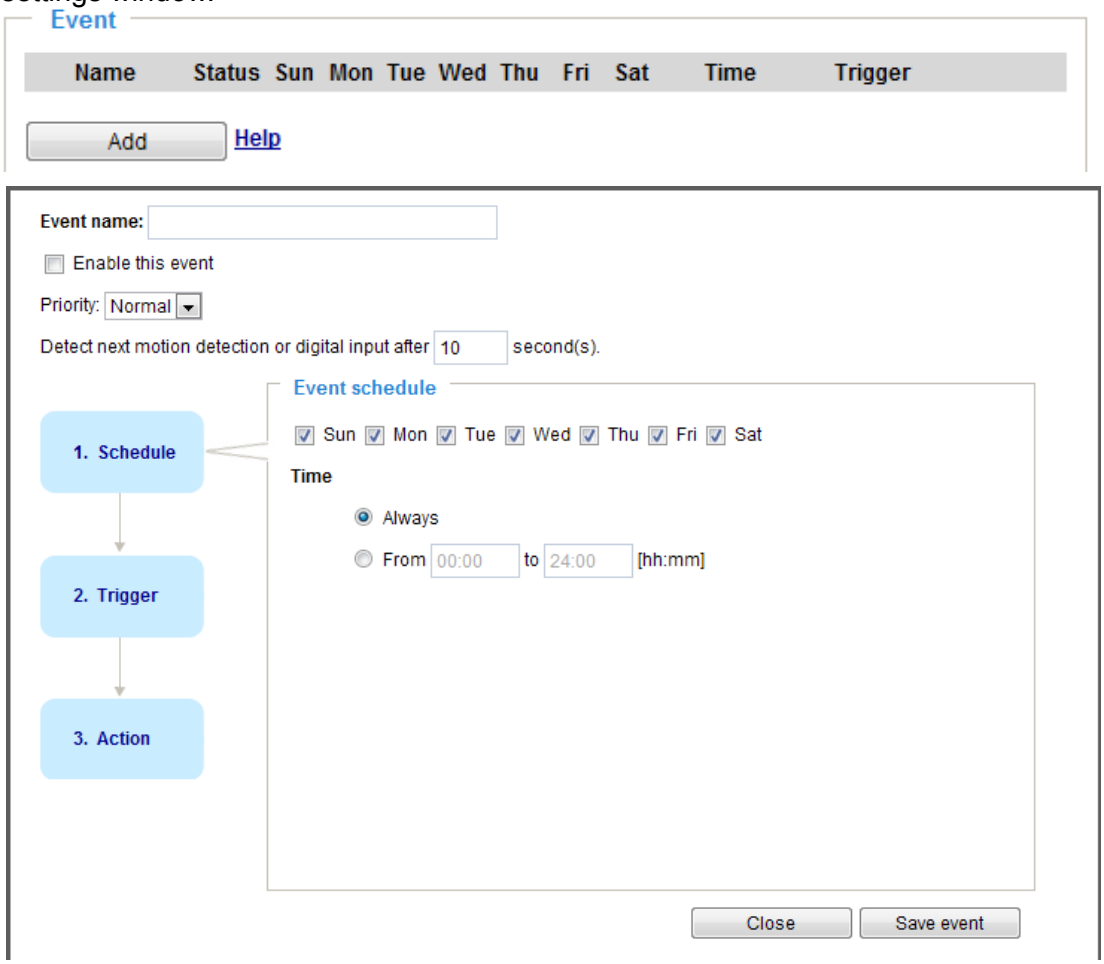
# Event > Event settings Advanced Mode

This section explains how to configure the Network Camera to respond to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to an FTP server or e-mail address as notifications. Click on **Help**, there is an illustration shown in the pop-up window explaining that an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action that will be performed.




## Event

An event is an action initiated by a user-defined trigger source. In the **Event** column, click **Add** to open the event settings window.



■ Event name: Enter a name for the event setting.

■ Enable this event: Select this checkbox to enable the event setting.

■ Priority: Select the relative importance of this event (High, Normal, or Low). Events with a higher priority setting will be executed first.

■ Detect next event after ☐ seconds: Enter the duration in seconds to pause motion detection after a motion is detected. This prevents too many events to be triggered within a short time.

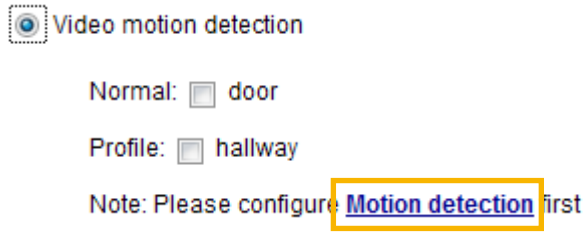
Follow the steps 1~3 to arrange the three elements -- Schedule, Trigger, and Action to set an event. A total of 3 event settings can be configured.

1. Schedule
Specify the period for the event. Please select the days of the week and the time in a day (in 24-hr time format) to specify when will the event-triggering conditions take effect.

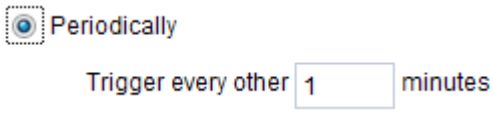
2. Trigger
This is the cause or stimulus which defines what will trigger the event. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital inputs.

There are several choices of trigger sources as shown below. Select each item to display its related options.

■ Video motion detection
This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to Motion Detection on page 117 for details.




■ Periodically
This option allows the Network Camera to trigger periodically for every other defined minute. Up to 999 minutes are allowed.

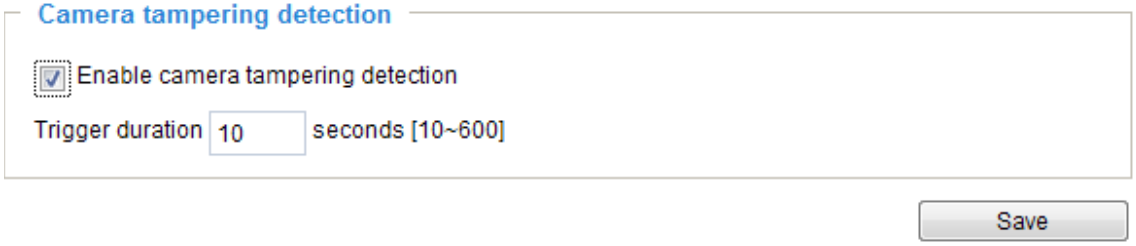



■ Digital input
This option allows the Network Camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices with digital input devices on the market which help detect changes in temperature, vibration, sound, light, etc.

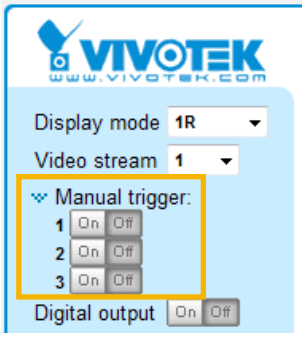
■ System boot
This option triggers the Network Camera when the power to the Network Camera is disconnected.

■ Recording notify
This option allows the Network Camera to trigger when the recording disk is full or when recording starts to overwrite older data.

■ Camera tampering detection
This option allows the Network Camera to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 120 for detailed information.




■ Manual Trigger
This option allows user to enable event triggers manually by clicking the on/off button on the homepage. Please configure 1 ~ 3 events before using this function.


3. Action
Define the actions to be performed by the Network Camera when a trigger is activated.


■ Trigger digital output for ☐ seconds
Select this option to turn on the external digital output device when a trigger is activated. Specify the length of the trigger interval in the text box.

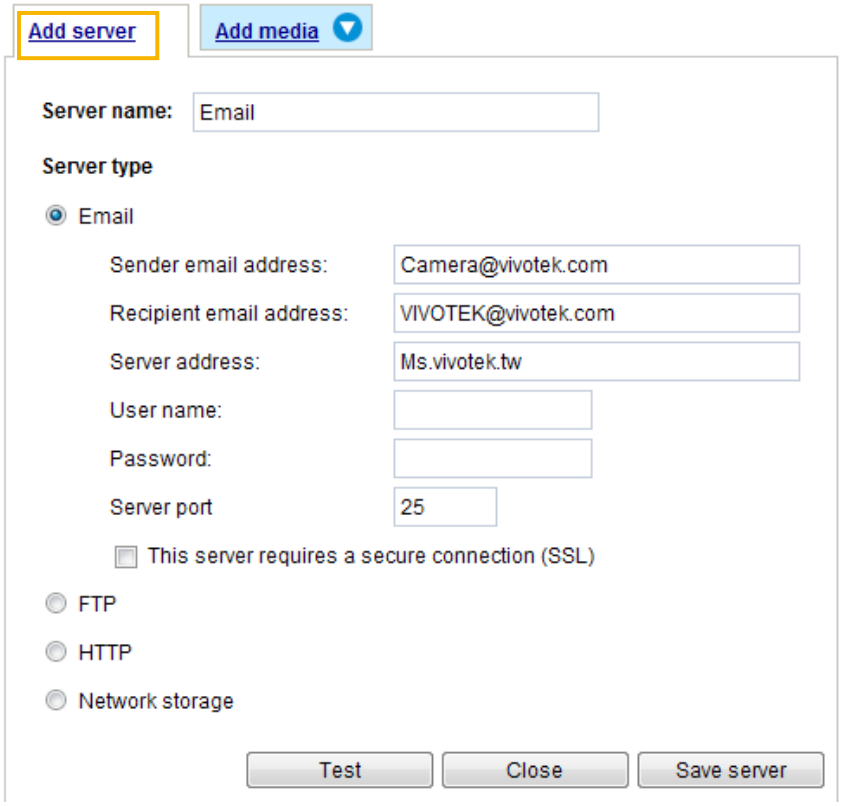
■ Backup media if the network is disconnected
Select this option to backup media file on SD card if the network is disconnected. Please note that this function will only apply after you set up the network storage (NAS). For more information about how to set up network storage, please refer to page 129.

To configure an event with video recording or snapshots, it is necessary to configure/provide servers and storage media settings so that the Network Camera will know where to send the media files to when a trigger is activated.

## Add server

Click **Add server** to unfold the server setting window. You can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item to display the detailed configuration options. You can configure either one or all of them.




Server type - Email
Select to send the media files via email when a trigger is activated.

■ Server name: Enter a name for the server setting.

■ Sender email address: Enter a valid email address as the sender address.

■ Recipient email address: Enter a valid email address as the recipient address.

■ Server address: Enter the domain name or IP address of the email server.

■ User name: Enter the user name of the email account if necessary.

■ Password: Enter the password of the email account if necessary.

■ Server port: The default mail server port is set to 25. You can also manually set another port.

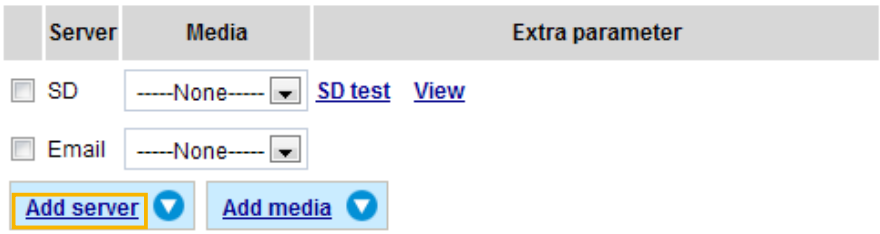
If your SMTP server requires a secure connection (SSL), check **This server requires a secure connection (SSL).**

To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will also receive an email indicating the result.



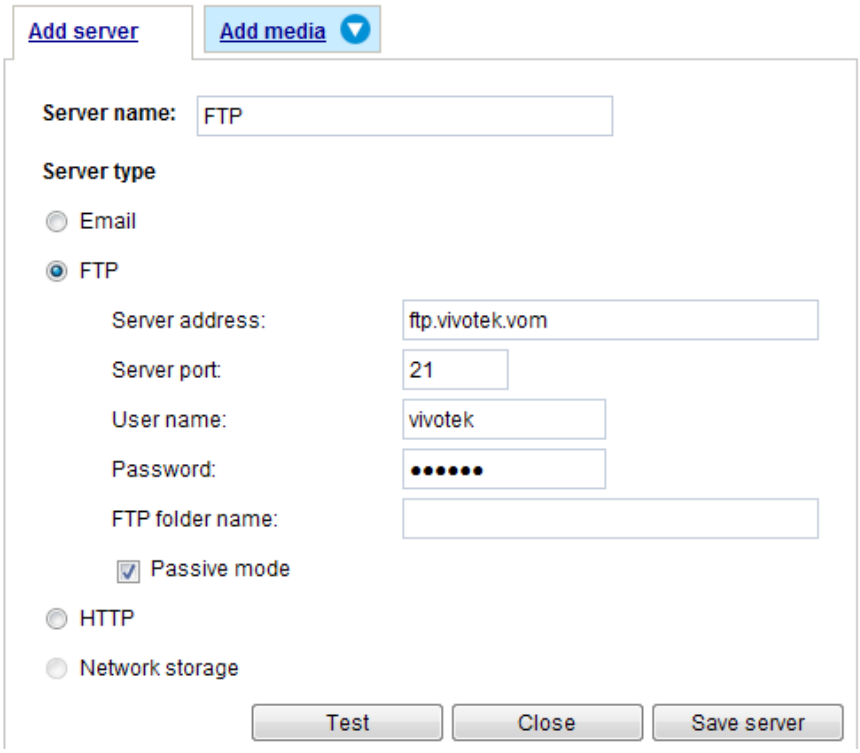
Click **Save server** to enable the settings, then click **Close** to exit the Add server page.

After you set up the first event server, a new item for event server will automatically appear on the Server list. If you wish to add more server options, click **Add server**.




Server type - FTP

Select to send the media files to an FTP server when a trigger is activated.




■ Server name: Enter a name for the server setting.

■ Server address: Enter the domain name or IP address of the FTP server.

■ Server port: By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.

■ User name: Enter the login name of the FTP account.

■ Password: Enter the password of the FTP account.

■ FTP folder name
Enter the folder where the media file will be placed. If the folder name does not exist, the Network Camera will create one on the FTP server.

■ Passive mode
Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as shown below. If successful, you will also receive a test.txt file on the FTP server.



Click **Save server** to enable the settings, then click **Close** to exit the Add server page.

Server type - HTTP
Select to send the media files to an HTTP server when a trigger is activated.


■ Server name: Enter a name for the server setting.

■ URL: Enter the URL of the HTTP server.

■ User name: Enter the user name if necessary.

■ Password: Enter the password if necessary.

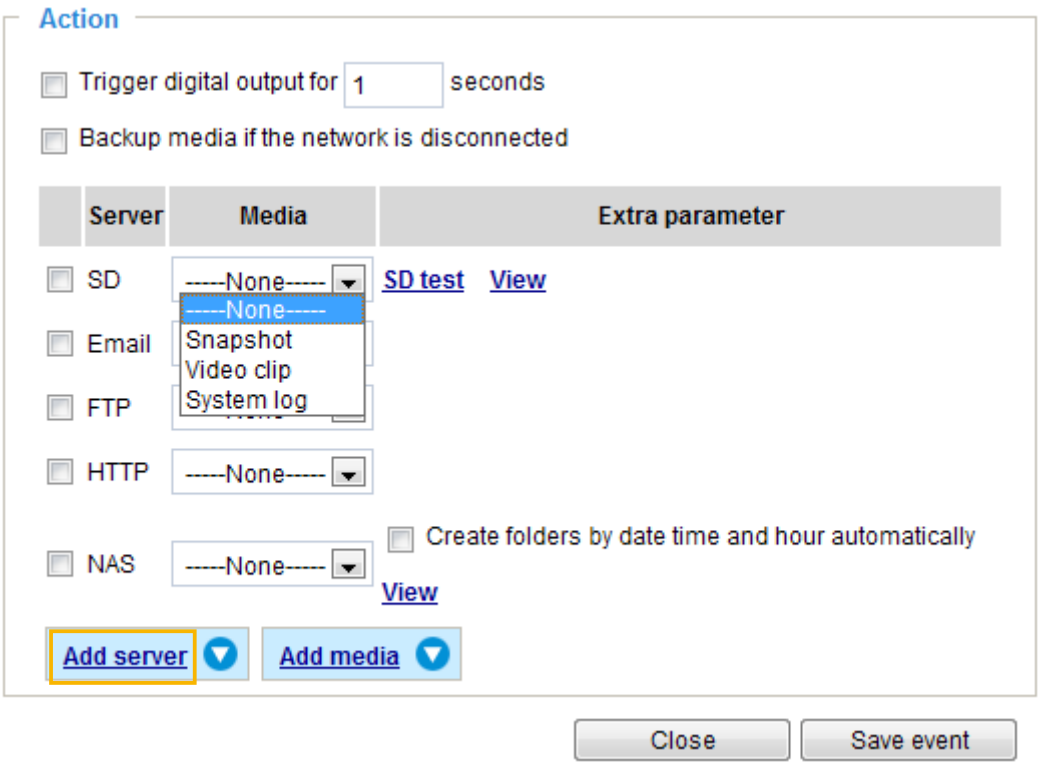
To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as below. If successful, you will receive a test.txt file on the HTTP server.



Click **Save server** to enable the settings and click **Close** to exit the Add server page.

Network storage:
Select to send the media files to a network storage location when a trigger is activated. Please refer to **NAS server** on page 129 for details.

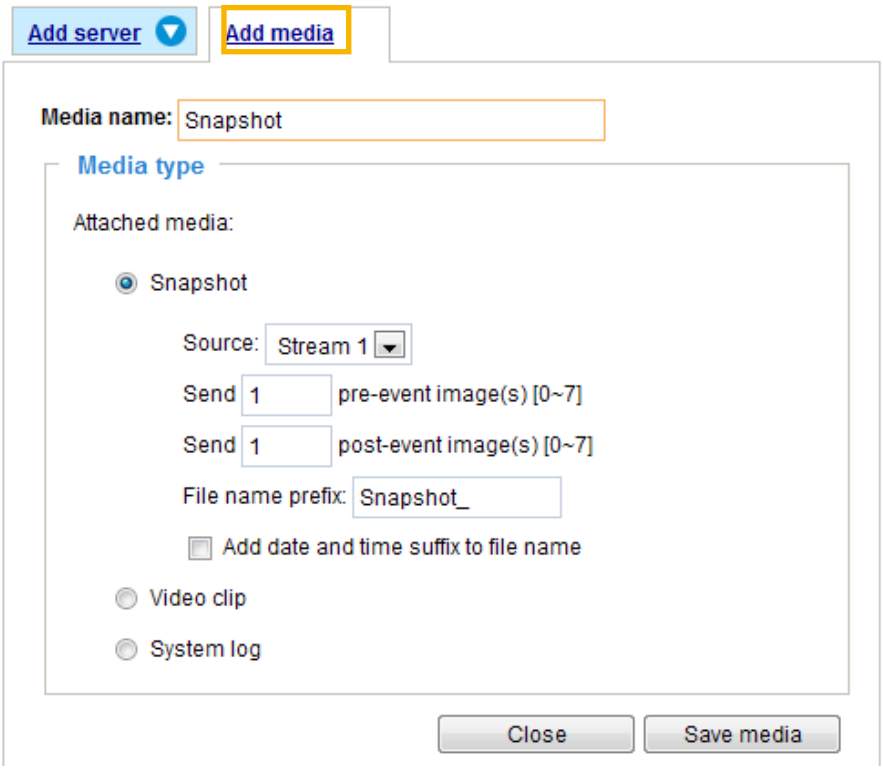
Click **Save server** to enable the settings, then click **Close** to exit the Add server page.




■ SD Test: Click to test your SD card. The system will display a message indicating success or failure. If you want to use your SD card for local storage, please format it before use. Please refer to page 132 for detailed information.

## Add media

Click **Add media** to open the media setting window. You can specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be configured. There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.




Media type - Snapshot
Select to send snapshots when a trigger is activated.

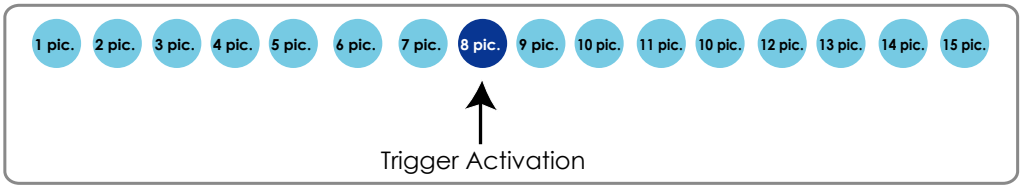
■ Media name: Enter a name for the media setting.

■ Source: Select to take snapshots from streams 1 ~ 3.

■ Send ☐ pre-event images
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

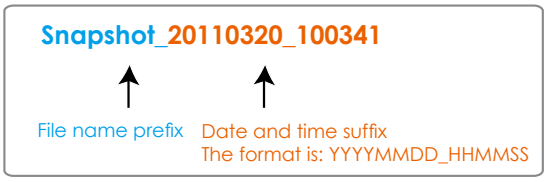
■ Send ☐ post-event images
Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images are generated after a trigger is activated.



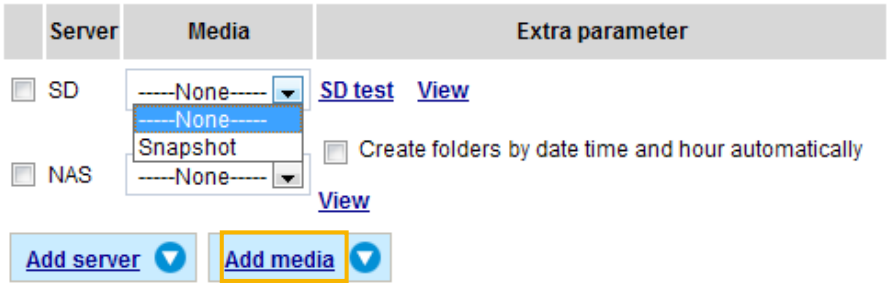

■ File name prefix
Enter the text that will be appended to the front of the file name.

■ Add date and time suffix to the file name. Select this option to add a date/time suffix to the file name. For example:

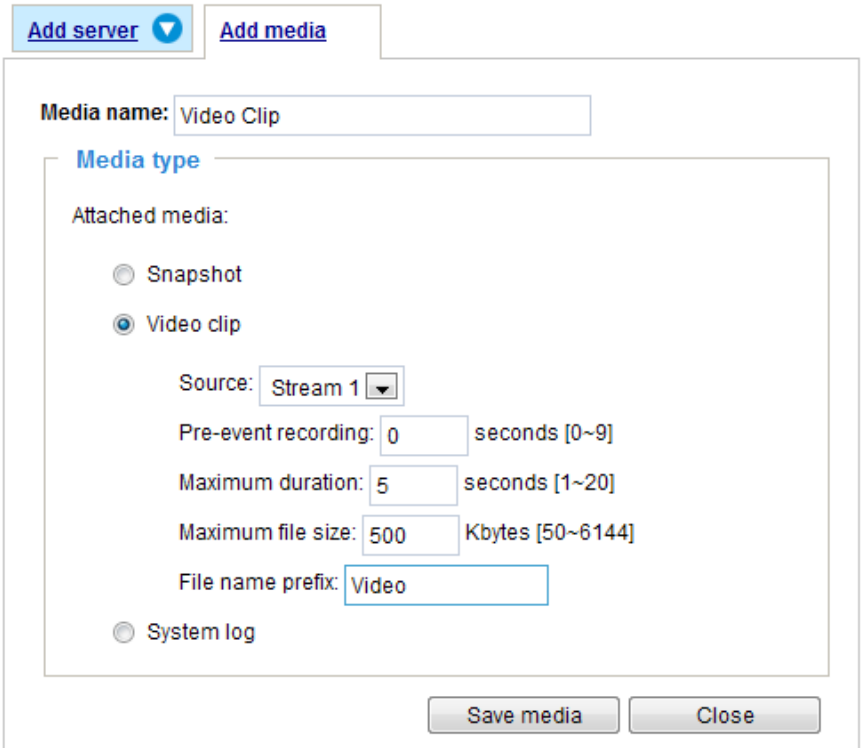



Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

After you set up the first media server, a new column for media server will automatically display on the Media list. If you wish to add more media options, click **Add media**.




Media type - Video clip
Select to send video clips when a trigger is activated.



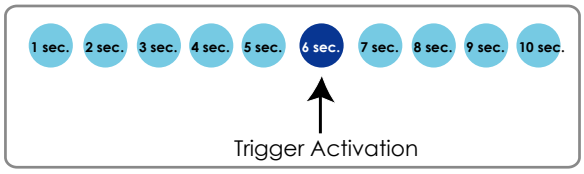

■ Media name: Enter a name for the media setting.

■ Source: Select the source of video clip.

■ Pre-event recording

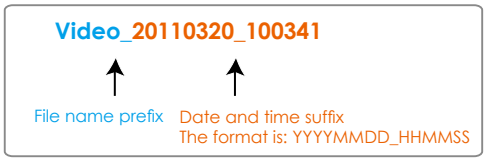
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds of video can be recorded.

■ Maximum duration
Specify the maximum recording duration in seconds. Up to 10 seconds of video can be recorded. For example, if pre-event recording is set to 5 seconds and the maximum duration is set to 10 seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.



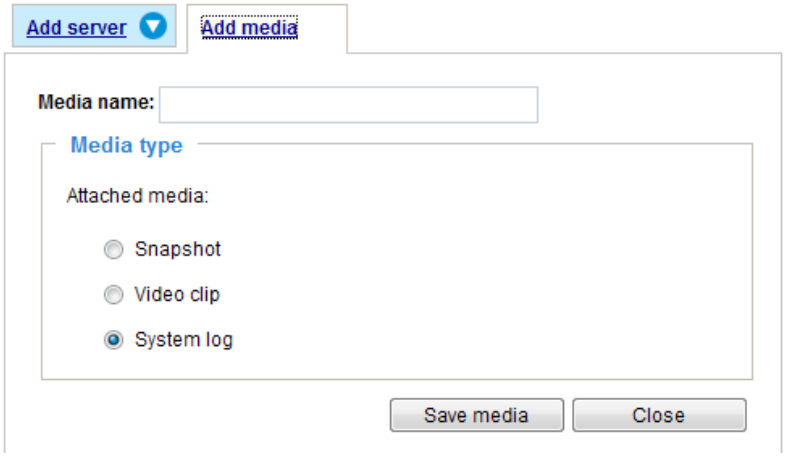

■ Maximum file size
Specify the maximum file size allowed.

■ File name prefix
Enter the text that will be appended to the front of the file name.
For example:

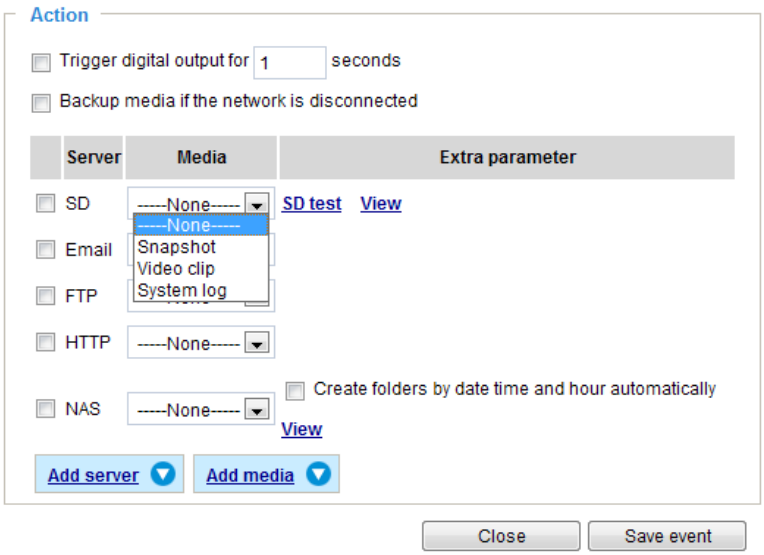



Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

Media type - System log
Select to send a system log when a trigger is activated.



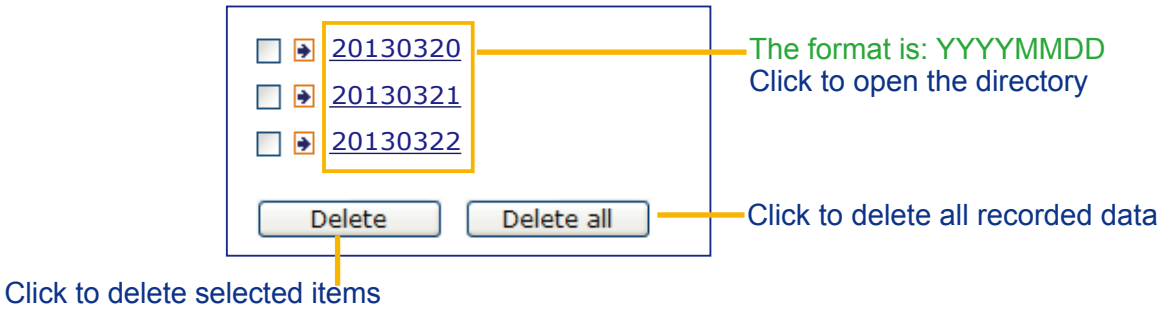

Click **Save media** to enable the settings, then click **Close** to exit the Add media page.



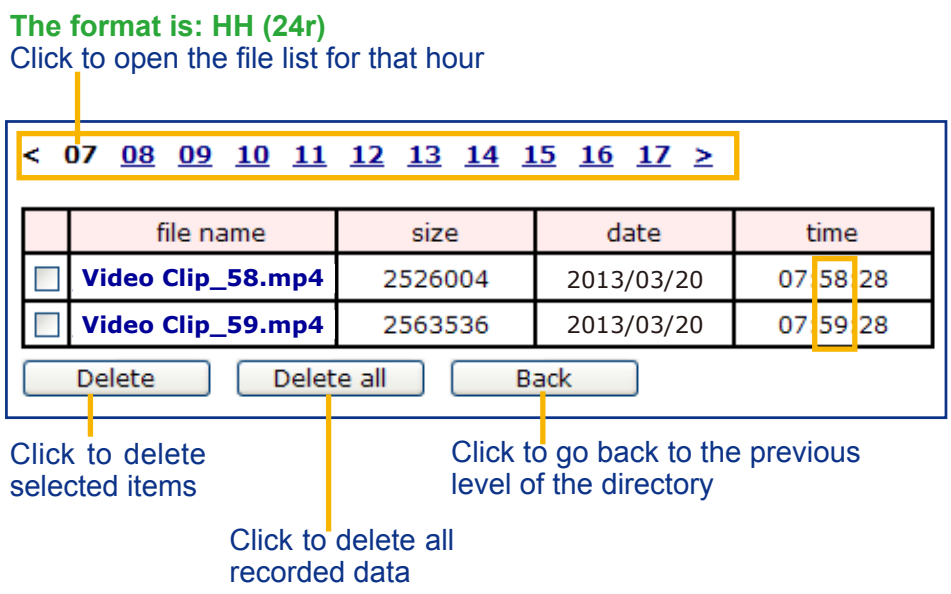
- View: Click this button to open a file list window. This function is only for SD card and Network Storage. If you click **View** button of SD card, a Local storage page will pop up for you to manage recorded files on SD card. For more information about Local storage, please refer to page 132. If you click **View** button of Network storage, a file directory window will pop up for you to view recorded data on Network storage.

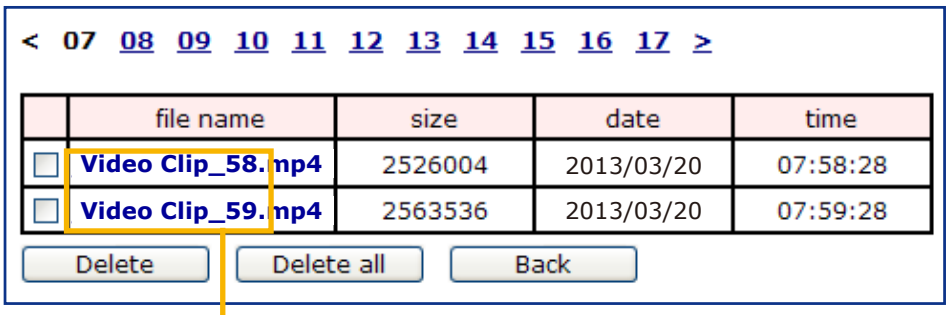
- Create folders by date, time, and hour automatically: If you check this item, the system will generate folders automatically by date.

The following is an example of a file destination with video clips:

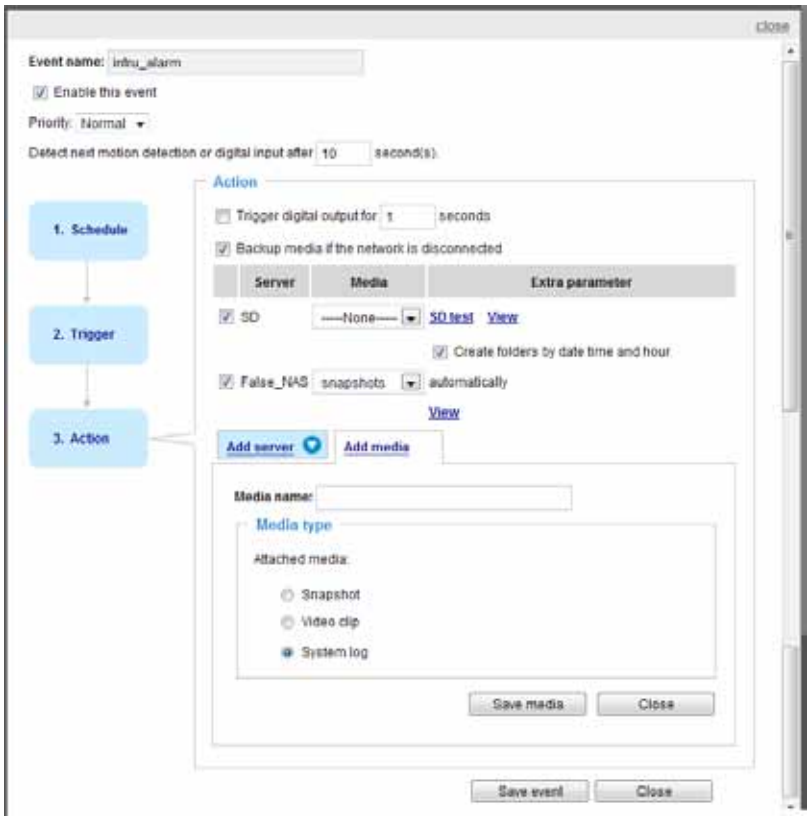



Click **20110320** to open the directory:



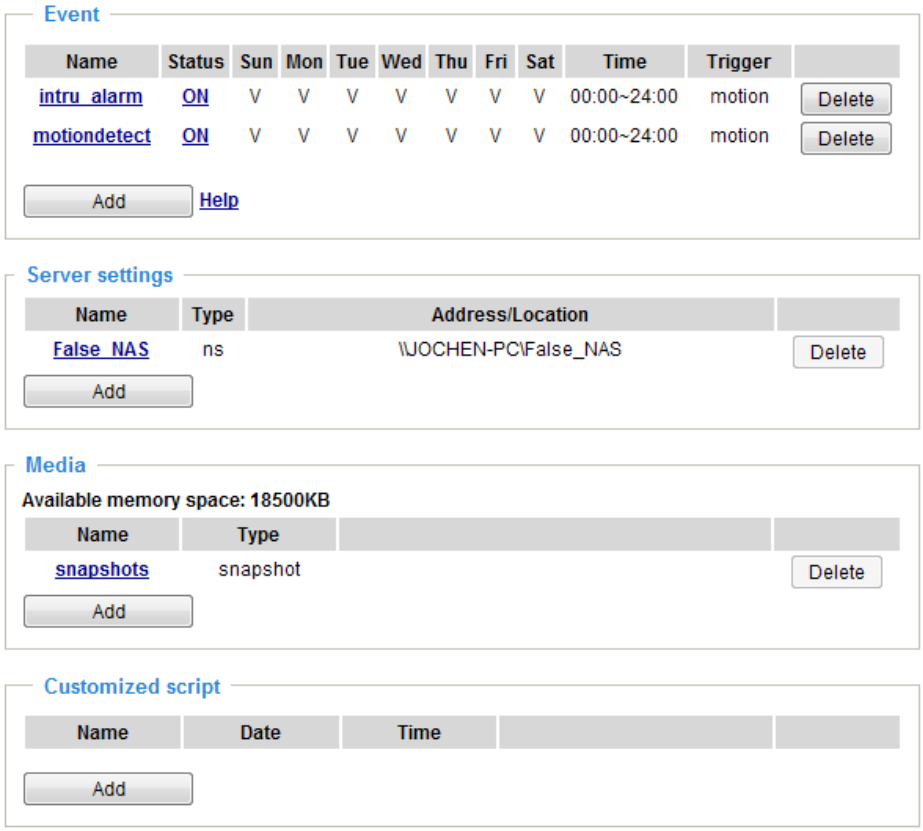



Here is an example of the Event setting:




When completed the settings with steps 1~3 to arrange Schedule, Trigger, and Action of an event, click **Save event** to enable the settings and click **Close** to exit the page.

The following is an example of the Event setting page:



When the Event Status is **ON**, once an event is triggered by motion detection, the Network Camera will automatically send snapshots via e-mail.

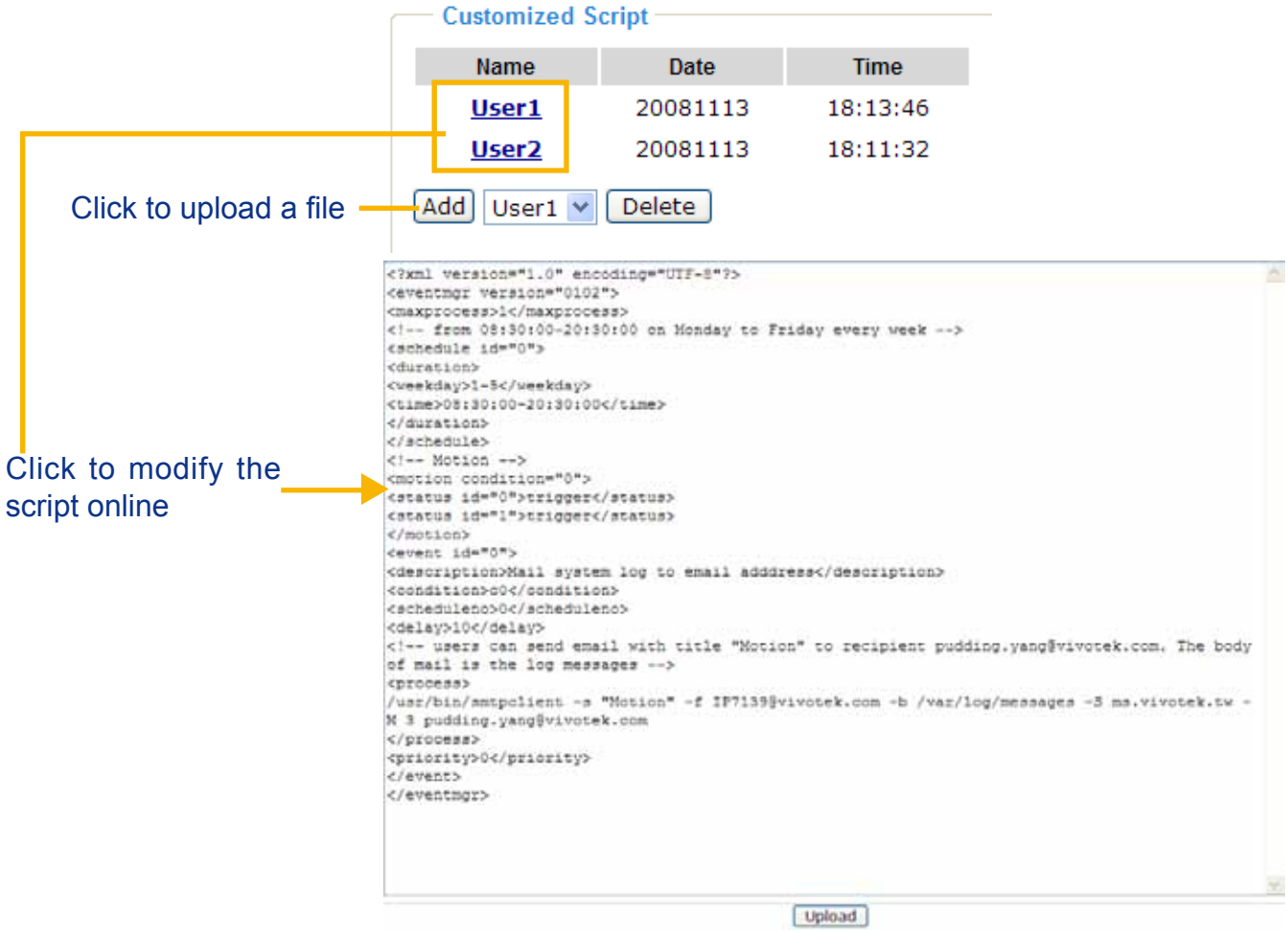
If you want to stop the event trigger, you can click **ON** to turn it to **OFF** status or click **Delete** to remove a previously-configured event setting.

To remove a server setting from the list, select a server name and click **Delete**. Note that only when the server setting is not being applied to an event setting can it be deleted.

To remove a media setting from the list, select a media name and click **Delete**. Note that only when the media setting is not being applied to an event setting can it be deleted.

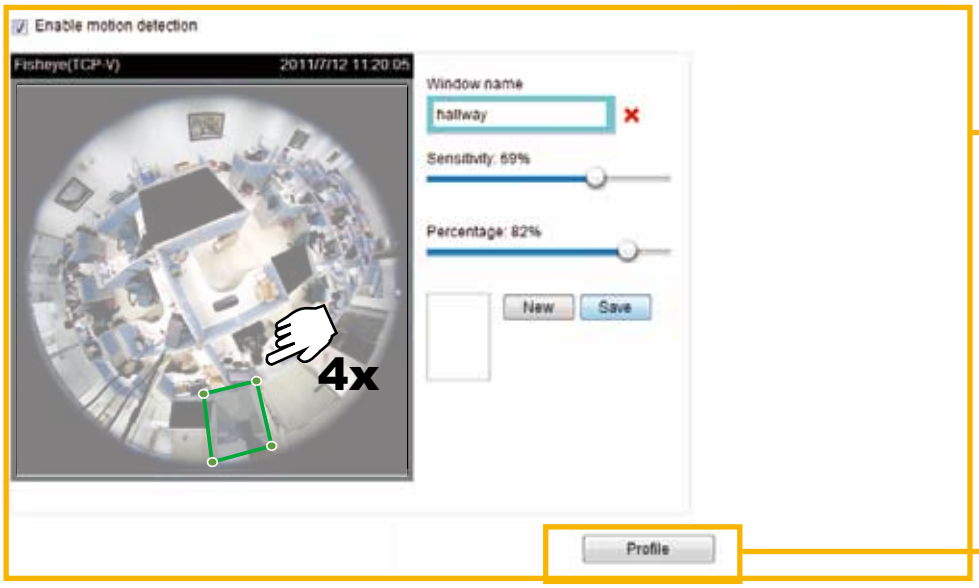
## Customized Script

This function allows you to upload a sample script (.xml file) to the webpage, which will save your time on configuring the settings. Please note that there is a limited number of customized scripts you can upload; if the current amount of customized scripts has reached the limit, an alert message will prompt. If you need more information, please contact VIVOTEK's technical support.



# Applications > Motion detection

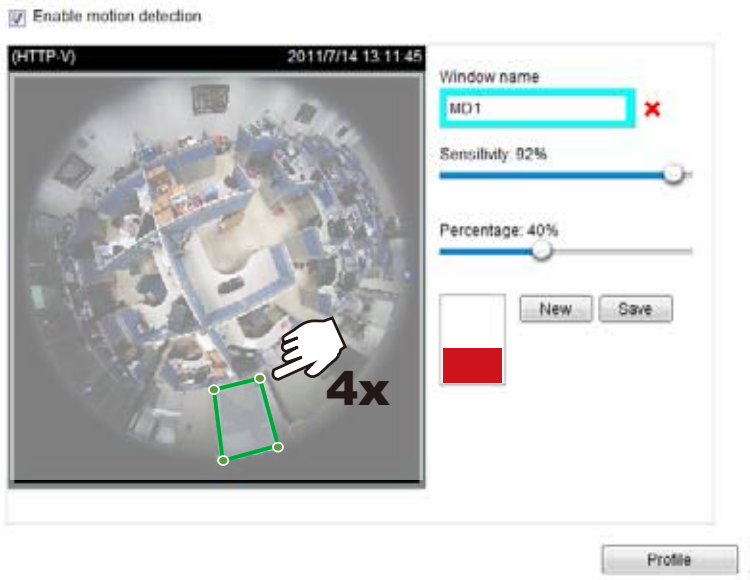
This section explains how to configure the Network Camera to enable motion detection. A total of five motion detection windows can be configured.




Follow the steps below to enable motion detection:

1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
   ■ Use four mouse clicks to define the area where Motion Detection will take effect.
   ■ To change the four points of the rectangular, place your mouse cursor on any of it until it turns into a four-direction mark ✣.
3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slide bar.
4. Click **Save** to enable the settings.
5. Select **Enable motion detection** to enable this function.

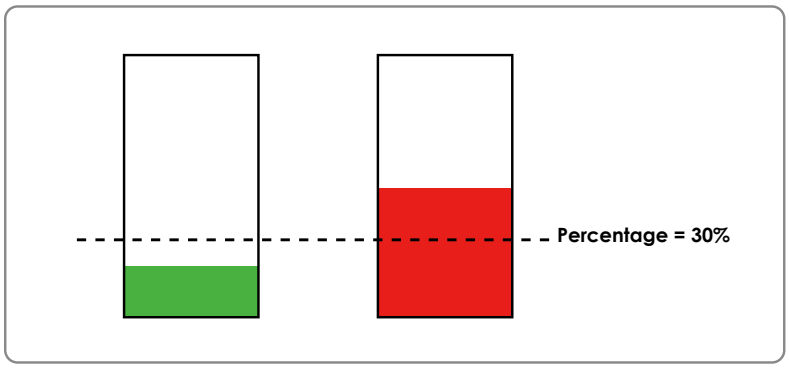
For example:



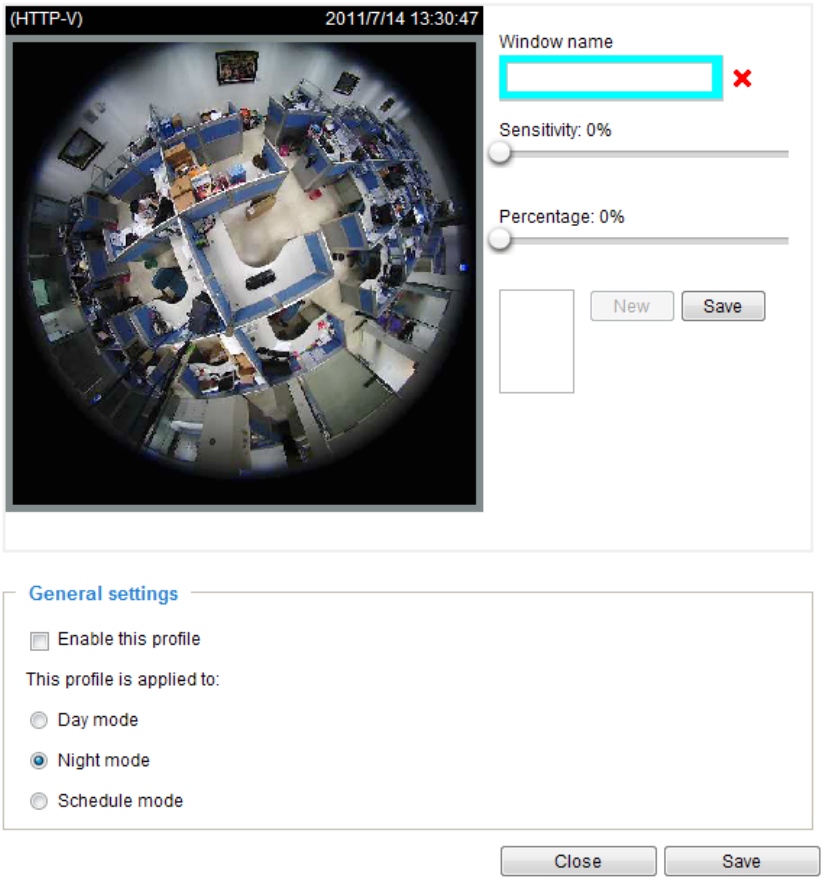

The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are considered to have exceeded the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to be sent to a remote server (Email, FTP) using this feature as a trigger source. For more information on how to set an event, please refer to Event settings

on page 104.

A green bar indicates that even though motions have been detected, the event has not been triggered because the image variations still fall under the defined threshold.




If you want to configure specific motion detection settings individually for day/night/schedule operations, please click **Profile** to open the Motion Detection Profile Settings page as shown below. A total of three motion detection windows can be configured on this page as well.

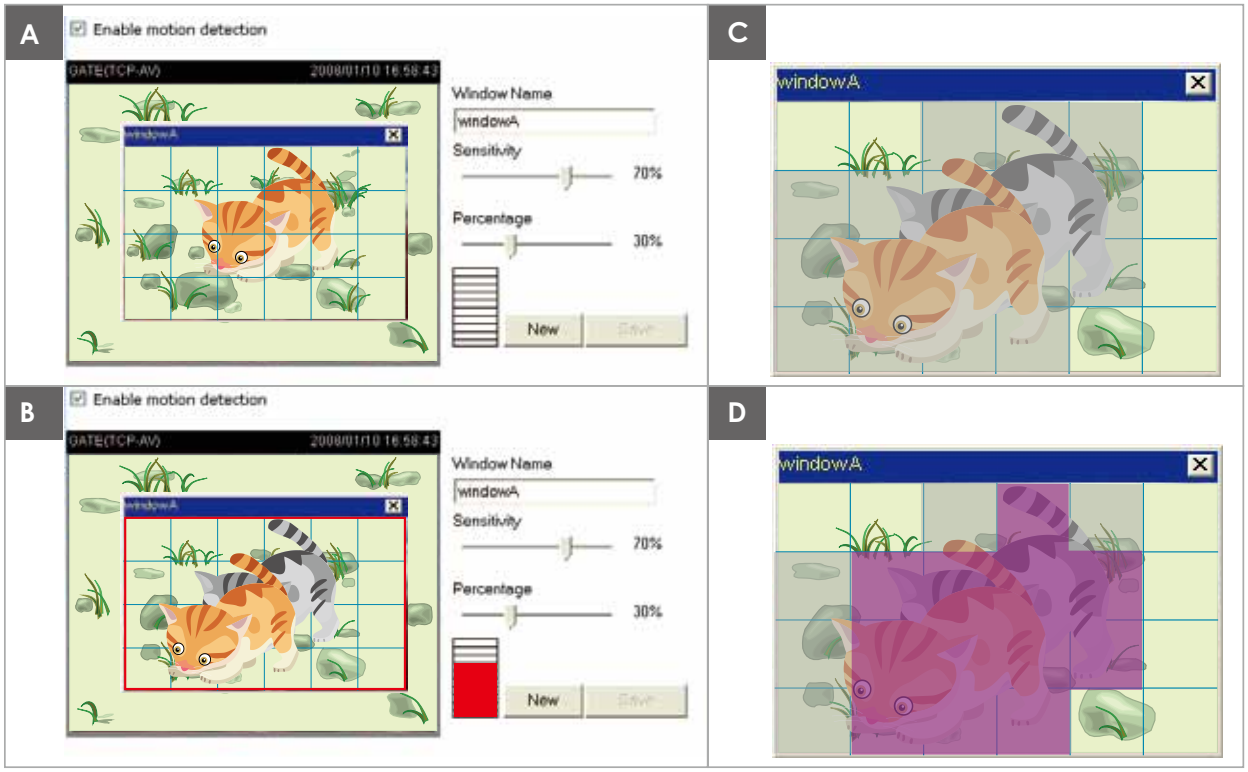



Please follow the steps beolw to set up a profile:
1. Create a new motion detection window.
2. Check **Enable this profile**.
3. Select the applicable mode: Day mode, Night mode, or Schedule mode. Please manually enter a time range if you prefer the Schedule mode.
4. Click **Save** to enable the settings and click **Close** to exit the page.

This motion detection window will also be displayed on the Event settings page. You can go to Event > Event settings > Trigger to choose it as a trigger source. Please refer to page 105 for detailed information.

**NOTE:**

► *How does motion detection work?*

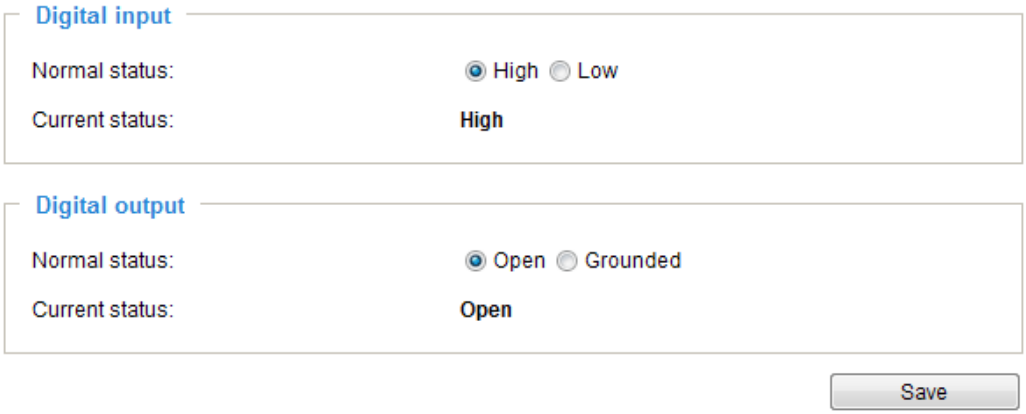



*There are two motion detection parameters: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C) and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to detect slight movements while smaller sensitivity settings will neglect them. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as "alerted pixels" (frame D).*

*Percentage is a value that expresses the proportion of "alerted pixels" to all pixels in the motion detection window. In this case, 50% of pixels are identified as "alerted pixels". When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will be outlined in red.*

*For applications that require a high level of security management, it is suggested to use **higher** sensitivity settings and **smaller** percentage values.*

## Applications > DI and DO Advanced Mode



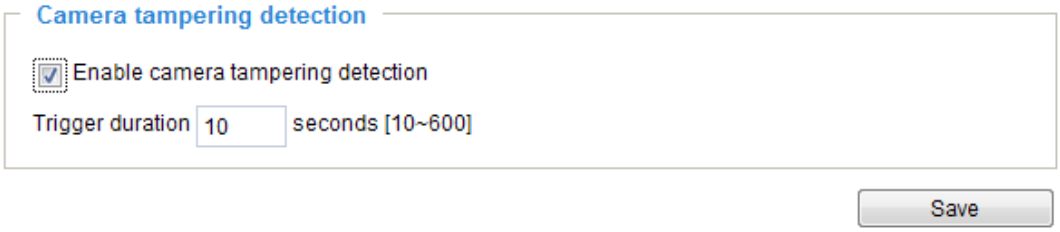

Digital input: Select High or Low as the Normal status for the digital input. Connect the digital input pin of the Network Camera to an external device to detect the current connection status.

Digital output: Select Grounded or Open to define the normal status for the digital output. Connect the digital output pin of the Network Camera to an external device to determine the current status.

Set up the event source as DI on **Event > Event settings > Trigger.** Please refer to page 105 for detailed information.

## Applications > Tampering detection

This section explains how to set up camera tamper detection. With tamper detection, the camera is capable of detecting incidents such as **redirection**, **blocking or defocusing**, or even **spray paint**.




Please follow the steps below to set up the camera tamper detection function:

1. Check **Enable camera tampering detection**.
2. Enter the tamper trigger duration. (10 sec. ~ 10 min.) The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold.
3. Set up the event source as Camera Tampering Detection on **Event > Event settings > Trigger.** Please refer to page 105 for detailed information.

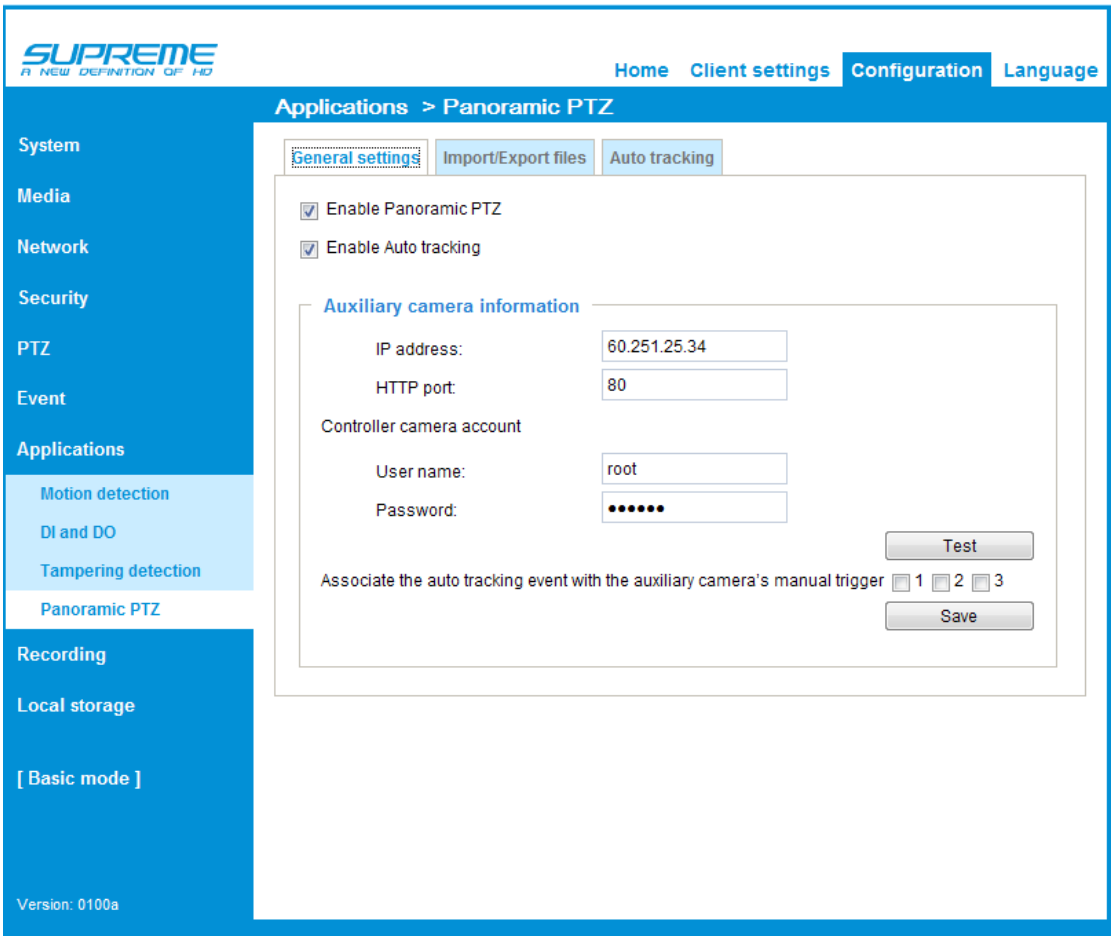
# Applications > Panoramic PTZ

**NOTE:**

The Panoramic PTZ configuration requires associated settings through the use of the **Calibration tool** software. You can skip this section and refer to the **Panoramic PTZ Installation Guide** for the complete procedure.

## Auto Tracking Configuration Steps

1. Open a web console with the "Controller" fisheye camera. When in the same subnet, use VIVOTEK's IW2 utility to locate the camera.
2. Access the Panoramic PTZ configuration page through Configuration > Applications > Panoramic PTZ.

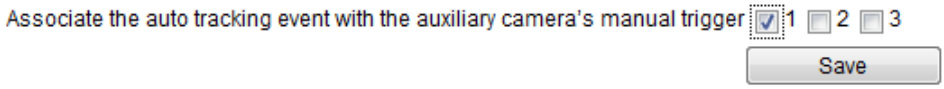


3. On the General settings pane, select both the "**Enable Panoramic PTZ**" and "**Enable Auto tracking**" checkboxes.

4. The Auxiliary camera information and the Controller camera account provide configuration options to the partner cameras in case that their IP addresses may be changed after the initial configuration. Use of static IPs is highly recommended in a Panoramic PTZ configuration. The **Test** button can be used to test the connectivity between the Controller and the Auxiliary cameras.

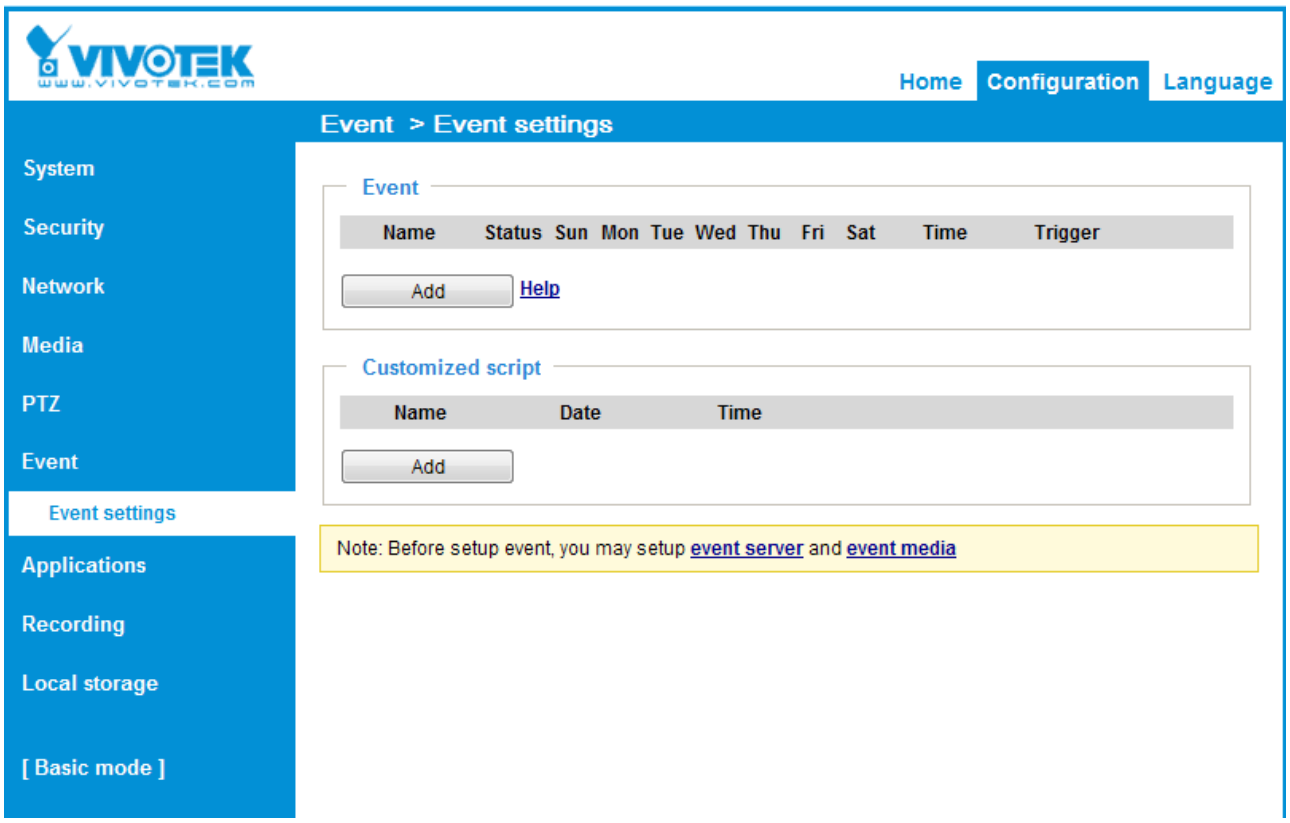
   Proceed with the following if you prefer recording the video while the speed dome is tracking an object:

   4-1. Select one or more **manual trigger** checkboxes, and click Save.



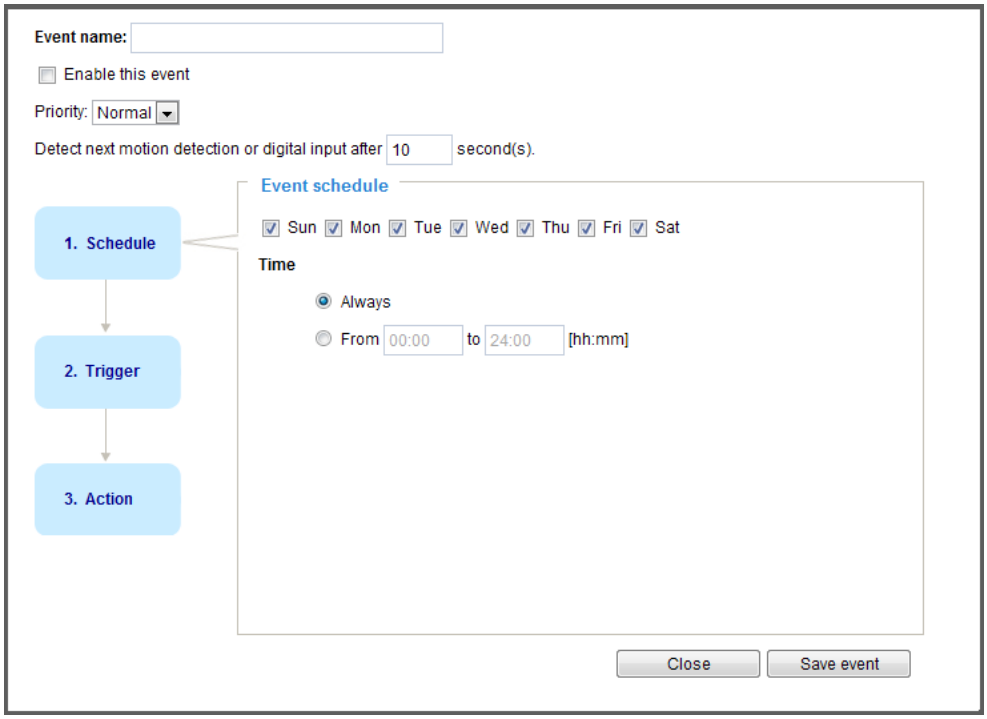

   4-2. Open a web console with the "Auxiliary" speed dome camera.

   4-3. Open the **Event** settings page through Configuration > Event > Event settings.



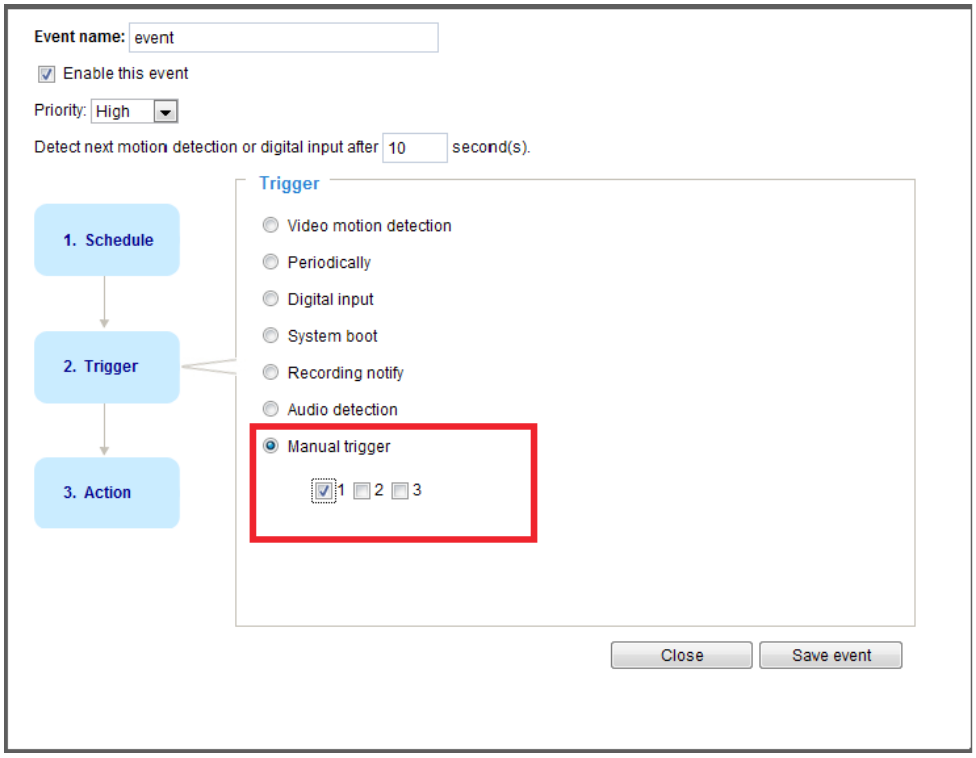

   4-4. Click **Add** to create a new event setting.

4-5. Enter an **Event name**, select the "**Enable this event**" checkbox, select the priority of the event, and if you prefer, configure the period of time during which this event setting will take effect .



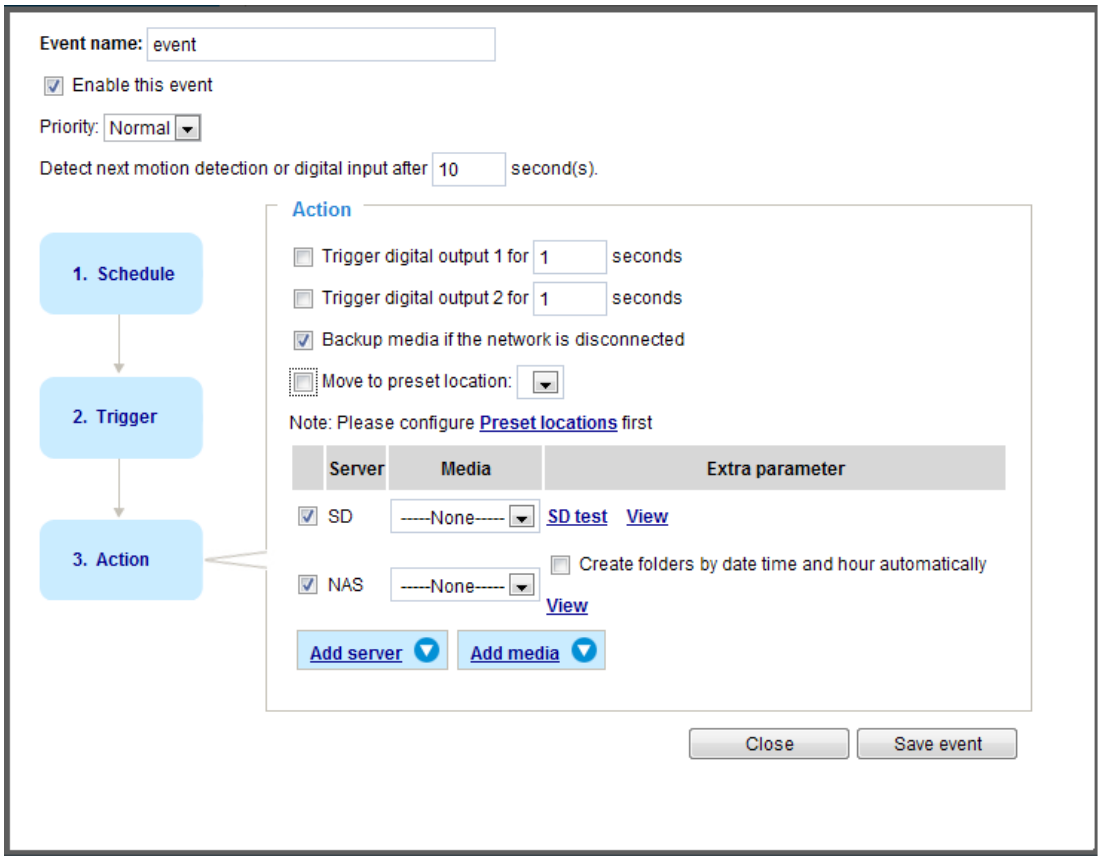

4-6. Click **Trigger** to open the Trigger page.

4-7. Select one of the checkboxes under "**Manual Trigger**" as the triggering cause.

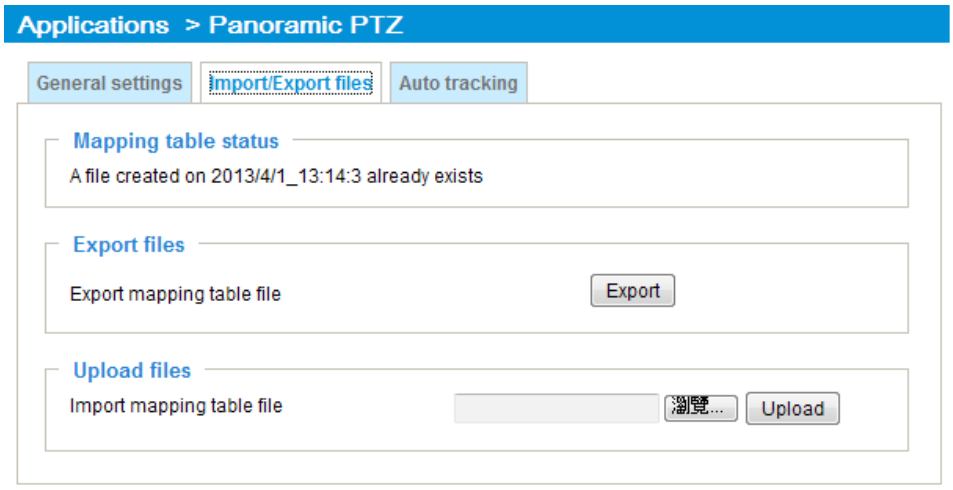



Note that the Manual trigger can last for another 10 seconds after the Controller (fisheye camera) returns to the normal state - no moving objects are detected.

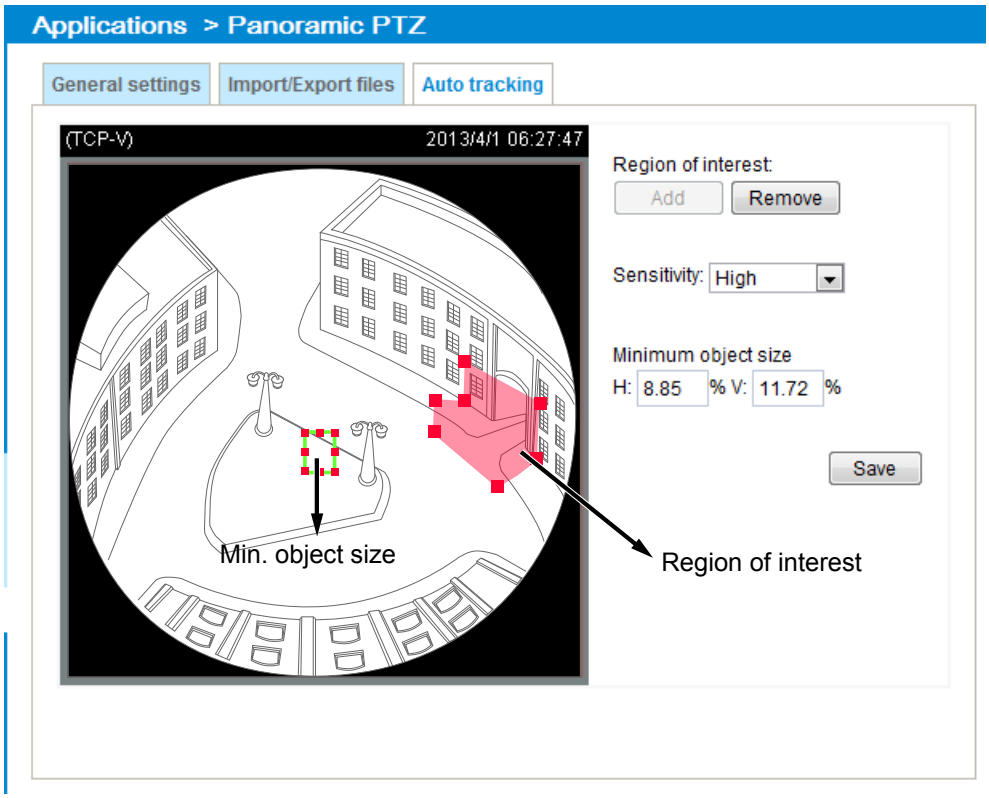
4-8. Click **Action** to open the Action page.
4-9. Configure the action to take by configuring recording to an SD card or a network attached storage. For more information about Event settings, please refer to the speed dome camera's User Manual.
4-10. Click **Save event** to preserve your configuration.




5. On the **Import/Export files** pane, you can see the mapping table information, export the current mapping table for backup purpose, or upload a configured table.



6. On the **Auto tracking** pane, you can create a region of interest and configure the triggering conditions for Auto tracking.
   - **By default, the region of interest is the full view.** Any objects entering the fisheye's field of view will trigger the tracking.
   - To configure a region of interest of your choice, click **Remove** and then click **Add** to create a new one.
   - You can then click on the screen, each click produces a red square (as a corner mark) to mark the area. Up to 20 red squares can be applied to mark an area of a complicated shape. **Double-click** on the screen to end the configuration process. Click and drag to change the corner marks' positions.
   - The green square in the middle of the screen indicates the minimum object size. Auto tracking will be activated **only if the objects entering the region are larger than the minimum size**. The smallest object size is 1.56% x1.56% of the fisheye's field of view. You can click and drag to resize, or drag the mini. size square to a place on the screen to compare and estimate the size of objects that might enter a region of interest.
   - You can also manually enter numbers in the percentage boxes to change the size of the minimum object size.




   - You can change the Sensitivity value using a pull-down menu. If you select a customized value, a slide bar will appear allowing you to change to a value between 0 and 100. The default is 30.

7. Click **Save** to preserve your configuration. Note that you can only configure one region of interest, and the speed dome can track one moving object at a time.

Since only one region of interest is allowed, as long as there is an existing region, the **Add** button will be unavailable.

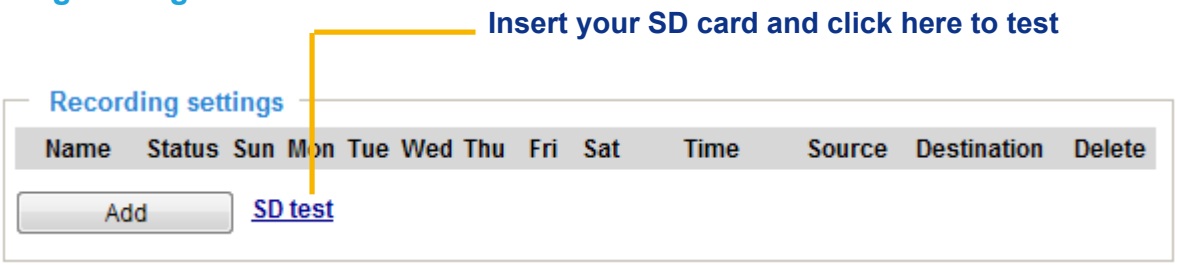
**NOTE:**

1. Auto tracking is configured on the fisheye camera, and the fisheye camera commands the speed dome camera to track an intruding object.
2. The speed dome can track one object at a time.
3. If multiple objects are present, the camera tracks the object that is farthest from the camera.
4. If a tracked object stays motionless for 10 seconds, camera will abandon it and start tracking another object that is farthest away from the center.
5. Camera will perform corresponding zoom in/out while tracking an object in order to contain just the silhouette of the moving object.
6. Installed at a position 6 meters from the ground, the configuration can track a moving object 60cm in width, in an area that is 10 meters in radius. When installed at a position 3 meters from the ground, the configuration can track a moving object 60cm in width, in an area that is 6 meters in radius.
7. Manual control (such as using a joystick to pan or tilt or using a click on VAST view cell) always has a higher priority than Auto tracking.

# Recording > Recording settings Advanced Mode

This section explains how to configure the recording settings for the Network Camera.

## Recording Settings

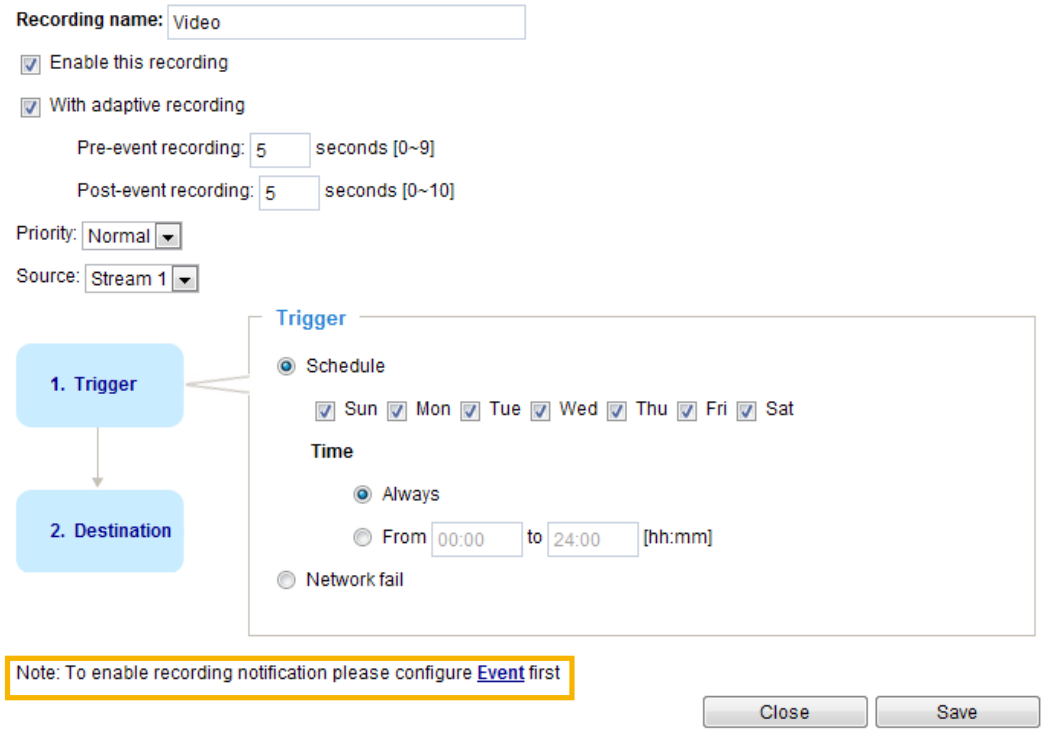



**NOTE:**

*Please remember to format your SD card when used for the first time. Please refer to page 132 for detailed information.*

### Recording Settings

Click **Add** to open the recording setting window. On this page, you can define the adaptive recording, recording source, recording schedule, and recording capacity. A total of 2 recording settings can be configured.

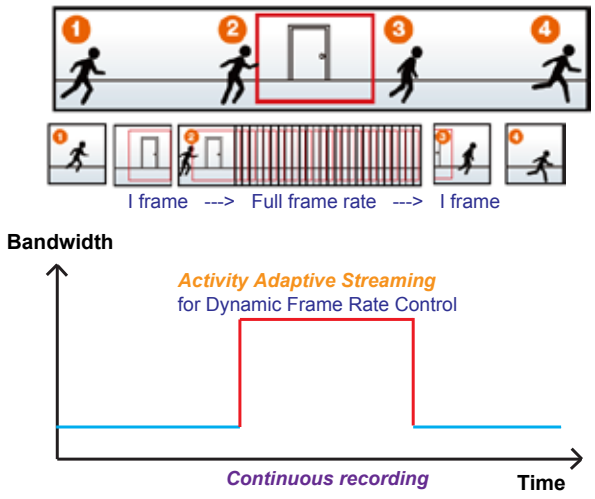



■ Recording name: Enter a name for the recording setting.

■ Enable this recording: Select this option to enable video recording.

■ With adaptive recording:
Select this option will activate the frame rate control according to alarm trigger. The frame control means that when there is a triggered alarm/event, the frame rate will raise up to the value you've set on the Stream setting page. Please refer to page 64 for more information.

If you enable adaptive recording on Camera A, only when an event is triggered on Camera A will the server record the streaming data in full frame rate; otherwise, it will only request the I frame data during normal monitoring, thus effectively save lots of bandwidths and storage.




**NOTE:**

► *To enable adaptive recording, please make sure you've set up the triggering sources such as Motion Detection, DI Device, or Manual Trigger.*

► *When there is no alarm trigger:*
*- JPEG mode: record 1 frame per second.*
*- H.264 mode: record the I frame only.*
*- MPEG-4 mode: record the I frame only.*

► *When the Intra frame period has been set to larger than >1s on Video settings page, the Intra frame period will be forced into 1s when the adaptive recording is activated.*

The alarm trigger includes: motion detection and DI detection. Please refer to Event settings on page 104.

■ Pre-event recording and post-event recording
The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before and after a trigger is activated.

■ Priority: Select the relative importance of this recording (High, Normal, or Low). Recording with a higher priority setting will be executed first.

■ Source: Select a stream for the recording source.

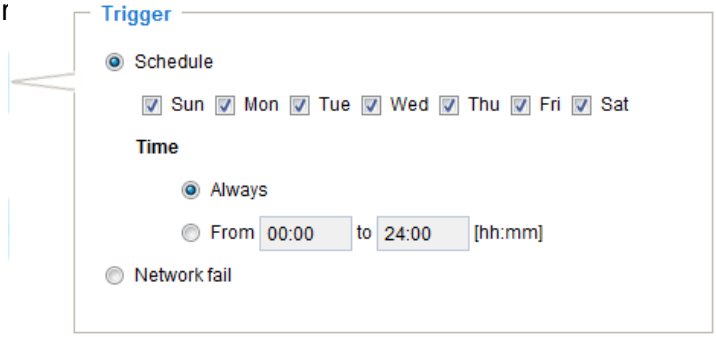
**NOTE:**

► *To enable adaptive recording, please also **enable time shift caching stream** and **select a caching stream** on Media > Video > Stream settings. Please refer to page 64 for detailed instruction.*

► *To enable recording notification please configure **Event settings** first. Please refer to page 104.*

Please follow steps 1~2 below to set up the recording:

1. Trigger
Select a trigger sour

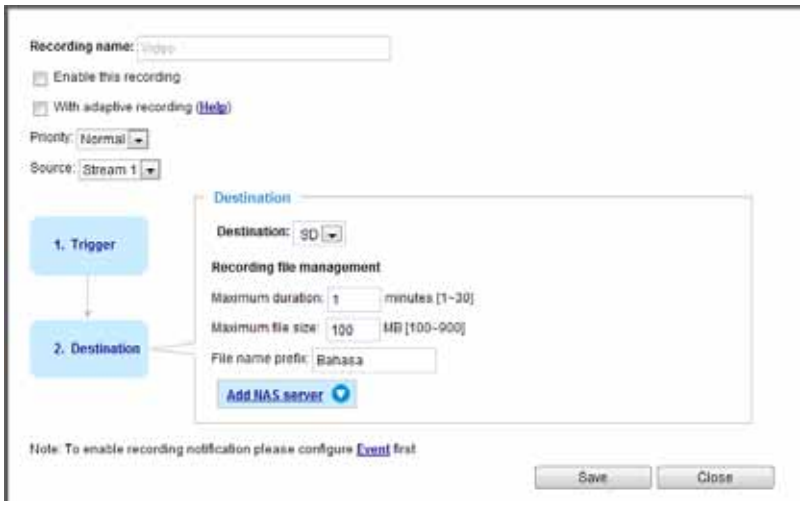



■ Schedule: The server will start to record files on the local storage or network attached storage (NAS).

■ Network fail: Since network fail, the server will start to record files onto the local storage (SD card).

2. Destination

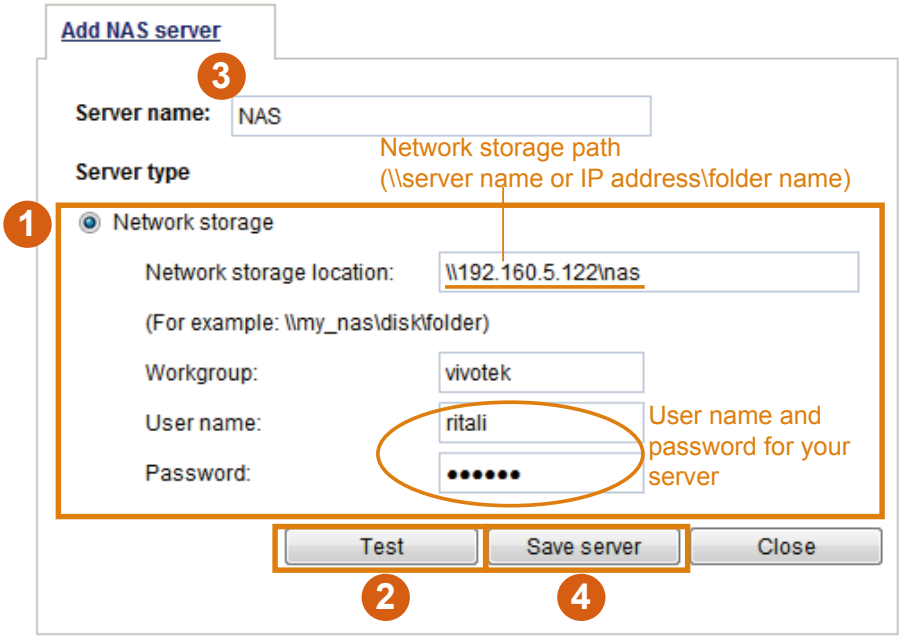
You can select the SD card or network storage (NAS) for the recorded video files.



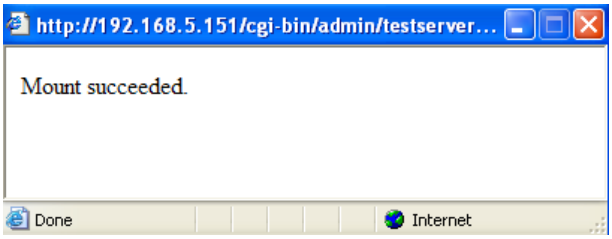

**NAS server**

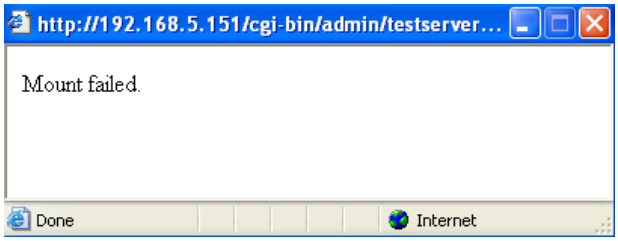
Click **Add NAS server** to open the server setting window and follow the steps below to set up:

1. Fill in the information for the access to the shared networked storage.
   For example:

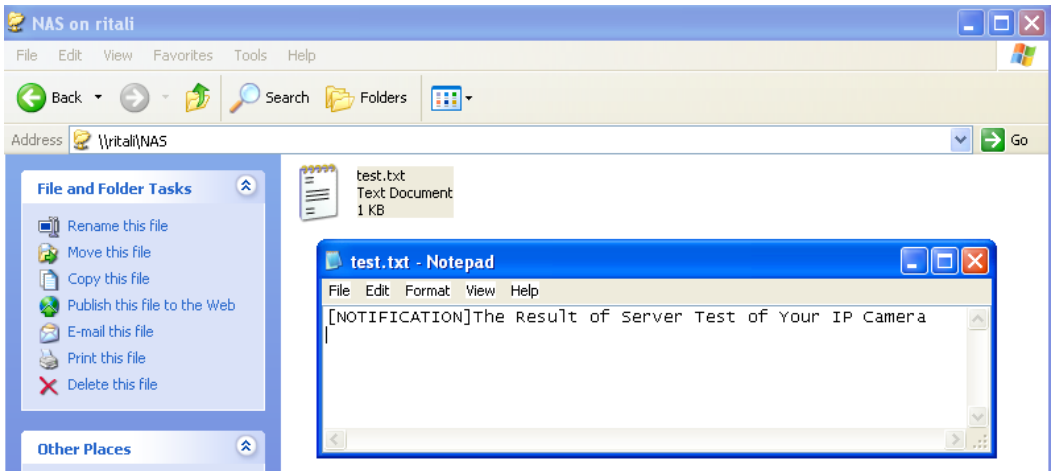



2. Click **Test** to check the setting. The result will be shown in the pop-up window.

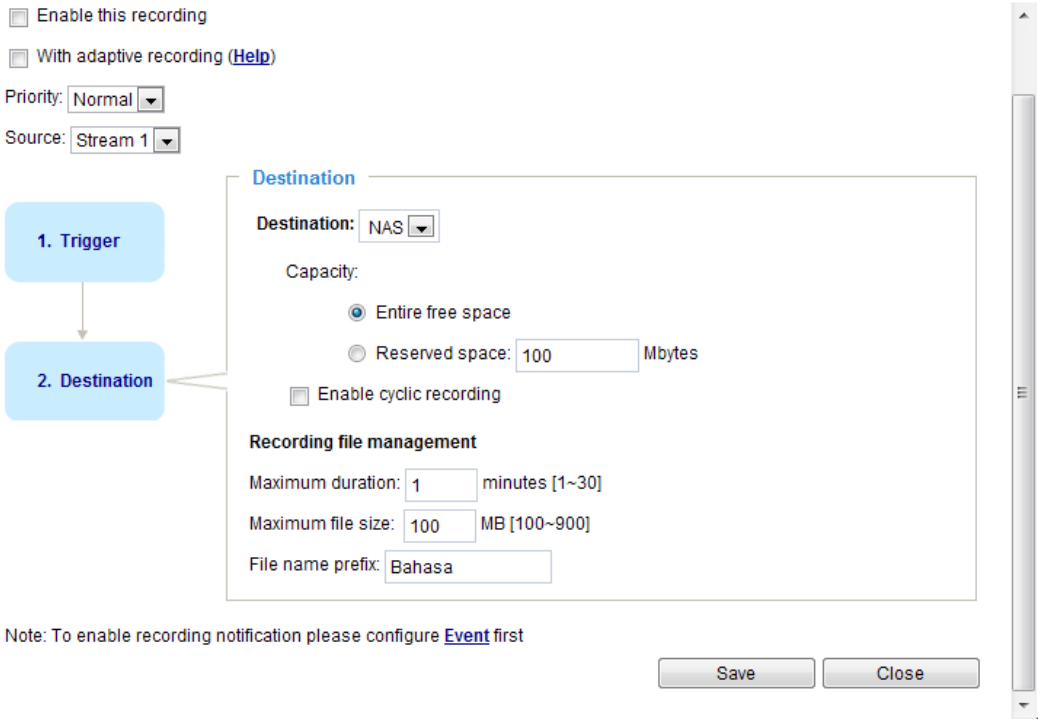


If successful, you will receive a test.txt file on the networked storage server.




3. Enter a server name.
4. Click **Save** to complete the settings and click **Close** to exit the page.




■ Capacity: You can either choose the entire available space or impose a reserved space. The **Reserved space** should be of the size of at least **15MBytes**. The reserved space can be used as a safe buffer especially when the cyclic recording function is enabled, during the transaction stage when a storage space is full and the incoming streaming data is about to overwrite the previously saved videos.

■ File name prefix: Enter the text that will be appended to the front of the file name.

■ Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one.

**Recording file management**

■ Maximum duration: This determines the length of each recorded video, applicable from 1 to 30 minutes.

■ Maximum file size: This determines the file size of each concluded recording. The applicable sizes

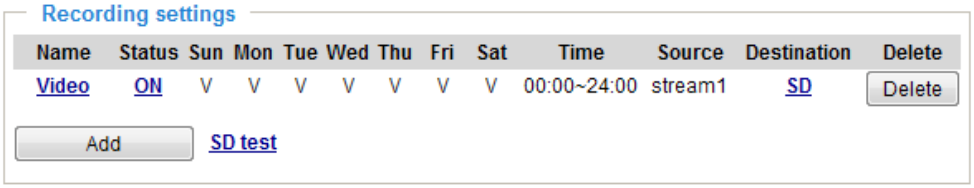
range from 100 to 900 Megabytes.

■ File name prefix: Enter a name for each recorded video.

If you want to enable recording notification, please click **Event** to set up. Please refer to **Event > Event settings** on page 104 for more details.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit this page. When the system begins recording, it will send the recorded files to the network storage or SD card. The new recording name will appear on the recording page as shown below.

To remove an existing recording setting from the list, single-click to select it and click **Delete**.




■ **Video (Name)**: Click to open the Recording settings page to modify.

■ **ON (Status)**: Click to manually adjust the Status. (**ON**: start recording; **OFF**: stop recording)

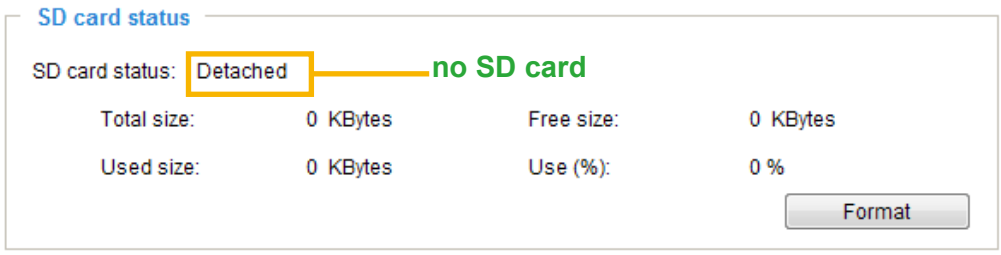
■ **NAS or SD (Destination)**: Click to open the file list of recordings as shown below. For more information about folder naming rules, please refer to page 114 for details.

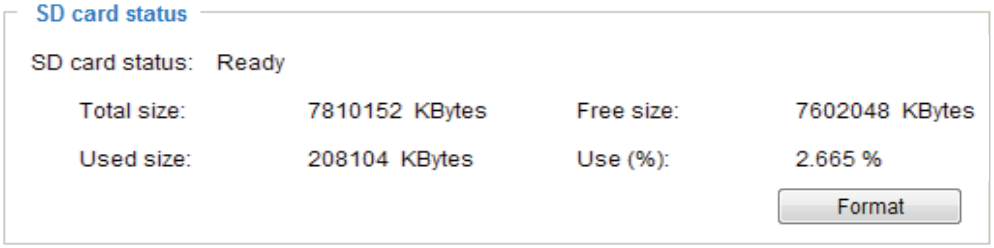
# Local storage > SD card management

This section explains how to manage the local storage on the Network Camera. Here you can view SD card status, and implement SD card control.

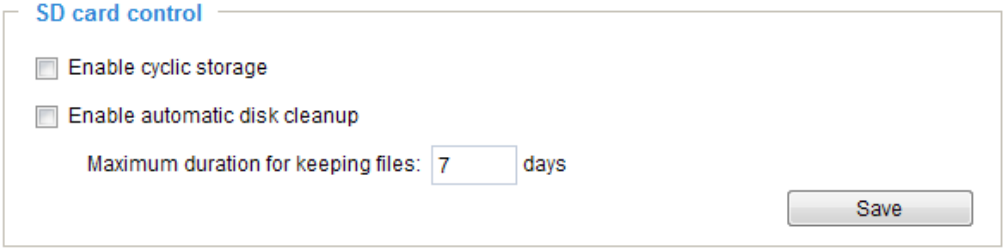
## SD card staus

This column shows the status and reserved space of your SD card. Please remember to format the SD card when using for the first time.




## SD card control




- Enable cyclic storage: Check this item if you want to enable cyclic recording. When recording uses up all capacity, the oldest file will be overwritten by the latest file.
- Enable automatic disk cleanup: Check this item and enter the number of days you wish to retain a file. For example, if you enter “7 days”, the recorded files will be stored on the SD card for 7 days.

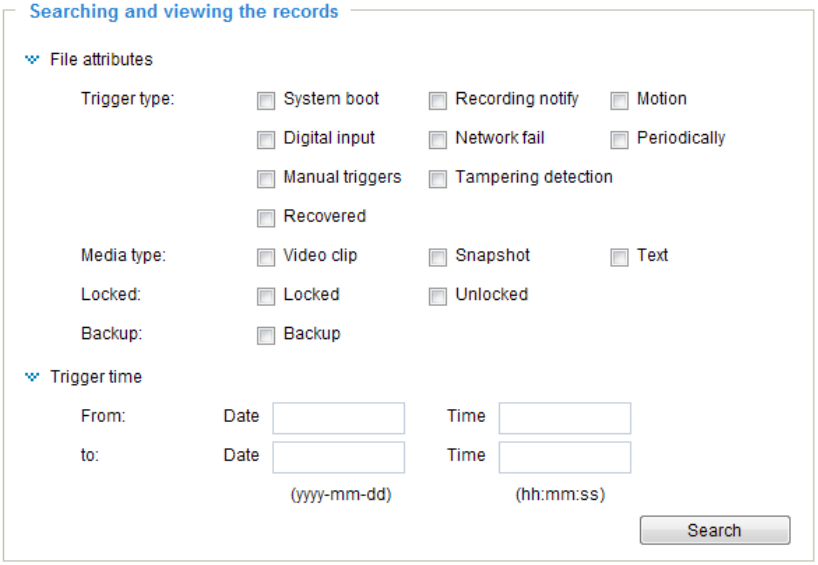
When all settings are completed, click **Save** to enable your settings.

# Local storage > Content management

This section explains how to manage the content of recorded videos on the Network Camera. Here you can search and view the records and view the searched results.

## Searching and Viewing the Records

This column allows the user to set up search criteria for recorded data. If you do not select any criteria and click **Search** button, all recorded data will be listed in the **Search Results** cloumn.




■ File attributes: Select one or more items as your search criteria.
■ Trigger time: Manually enter the time range you want to search.

Click **Search** and the recorded data corresponding to the search criteria will be listed in **Search Results** window.

**IMPORTANT:**

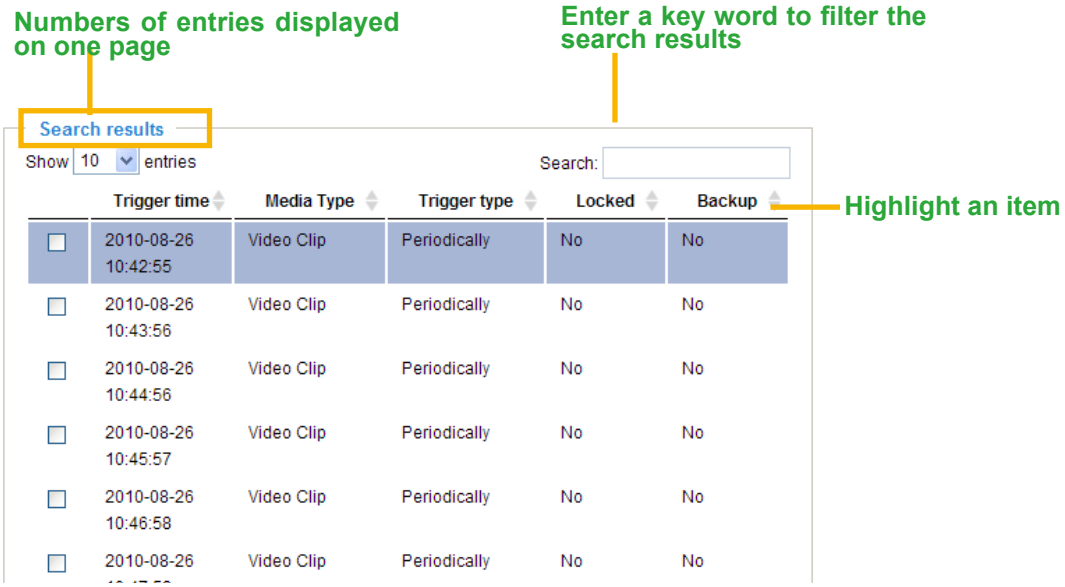
Due to the limitations of file system and video recording format, a video recording interrupted by sabotage or power outage will produce inaccessible video fragments. And the loss of video makes it difficult to identify who sabotaged the camera and the assets it aims to protect.

This revision of firmware (0100d0 and above) supports "**Recoverable Recording**," a feature that enables the usability of video footages taken immediately before (less than 1 second) an interruption. By inserting meta tags and pointers to videos, videos recorded to the onboard SD card or networked storage is viewable even when it is abnormally discontinued. Some video frames will still be lost, yet it is now possible to retrieve important footages taken before a camera is destroyed or its power disconnected.

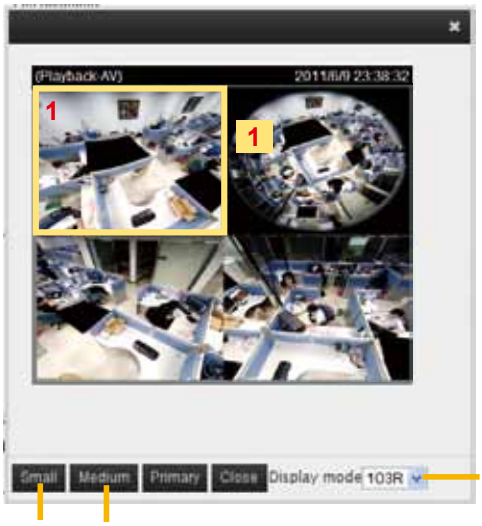
You can select the **Recovered** checkbox to search for the videos particularly affected by an interruption.

## Search Results

The following is an example of search results. There are four columns: Trigger time, Media type, Trigger type, and Locked. Click ⇕ to sort the search results in either direction.



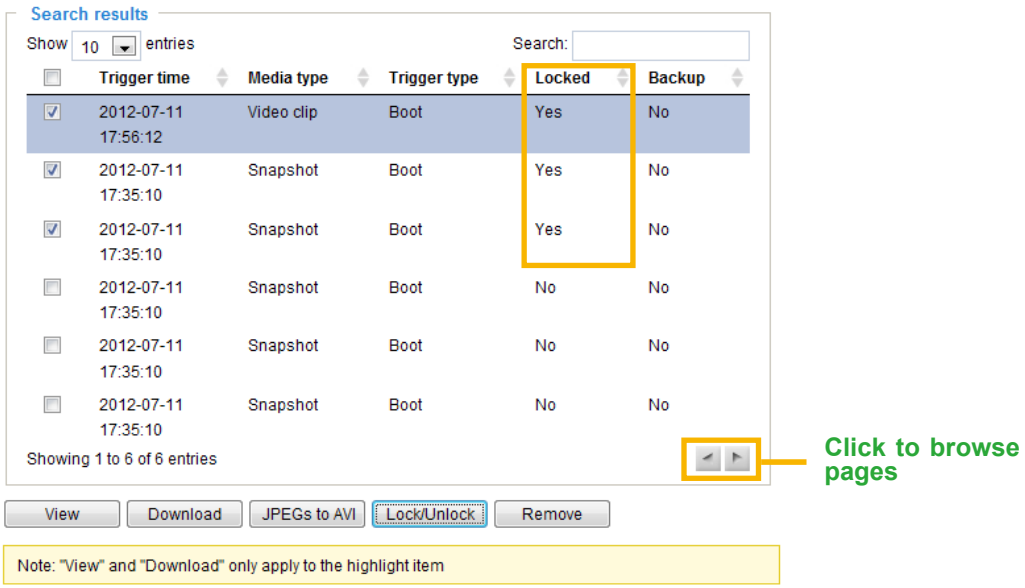

■ View: Click on a search result which will highlight the selected item in purple as shown above. Click the **View** button and a media window will pop up to play back the selected file.
For example:




■ Download: Click on a search result to highlight the selected item in purple as shown above. Then click the **Download** button and a file download window will pop up for you to save the file.

- JPEGs to AVI: This function only applies to “JPEG“ format files such as snapshots. You can select several snapshots from the list, then click this button. Those snapshots will be converted into an AVI file.

- Lock/Unlock: Select the desired search results, then click this button. The selected items will become Locked, which will not be deleted during cyclic recoroding. You can click again to unlock the selections. For example:




- Remove: Select the desired search results, then click this button to delete the files.

# Appendix

## URL Commands for the Network Camera

## 1. Overview

For some customers who already have their own web site or web control application, the Network Camera/Video Server can be easily integrated through URL syntax. This section specifies the external HTTP-based application programming interface. The HTTP-based camera interface provides the functionality to request a single image, control camera functions (PTZ, output relay etc.), and get and set internal parameter values. The image and CGI-requests are handled by the built-in Web server.

## 2. Style Convention

In URL syntax and in descriptions of CGI parameters, text within angle brackets denotes content that is to be replaced with either a value or a string. When replacing the text string, the angle brackets should also be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example further down in the page.

URL syntax is denoted with the word "Syntax:" written in bold face followed by a box with the referenced syntax as shown below. For example, name of the server is written as <servername> and is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam.adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg
```

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data is returned in HTTP format, i.e., each line is separated with a Carriage Return and Line Feed (CRLF) printed as \r\n.

Return:

```
HTTP/1.0 <HTTP code> <HTTP text>\r\n
```

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

**Example:** request a single snapshot image

```
http://mywebserver/cgi-bin/viewer/video.jpg
```

# 3. General CGI URL Syntax and Parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, these parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in functionally-related directories under the cgi-bin directory. The file extension .cgi is required.

Syntax:

| |
|---|
| http://<*servername*>/cgi-bin/<*subdir*>[/<*subdir*>...]/<*cgi*>.<*ext*><br>[?<parameter>=<value>[&<parameter>=<value>...]] |

**Example:** Set digital output #1 to active

http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1

# 4. Security Level

| SECURITY LEVEL | SUB-DIRECTORY | DESCRIPTION |
|---|---|---|
| 0 | anonymous | Unprotected. |
| 1 [view] | anonymous, viewer, dido, camctrl | 1. Can view, listen, talk to camera.<br>2. Can control DI/DO, PTZ of the camera. |
| 4 [operator] | anonymous, viewer, dido, camctrl, operator | Operator access rights can modify most of the camera's parameters except some privileges and network options. |
| 6 [admin] | anonymous, viewer, dido, camctrl, operator, admin | Administrator access rights can fully control the camera's operations. |
| 7 | N/A | Internal parameters. Unable to be changed by any external interfaces. |

# 5. Get Server Parameter Values

**Note:** The access right depends on the URL directory.

**Method:** GET/POST

Syntax:

| |
|---|
| http://<*servername*>/cgi-bin/anonymous/getparam.cgi?[<*parameter*>]<br>[&<parameter>…]<br><br>http://<*servername*>/cgi-bin/viewer/getparam.cgi?[<*parameter*>] |

[&<parameter>…]

http://<*servername*>/cgi-bin/operator/getparam.cgi?[<*parameter*>]
[&<parameter>…]

http://<*servername*>/cgi-bin/admin/getparam.cgi?[<*parameter*>]
[&<parameter>…]

Where the <*parameter*> should be <*group*>[_<*name*>] or <*group*>[.<*name*>]. If you do not specify any parameters, all the parameters on the server will be returned. If you specify only <*group*>, the parameters of the related group will be returned.

When querying parameter values, the current parameter values are returned.
A successful control request returns parameter pairs as follows:
Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<*parameter pair*>

where <parameter pair> is
<parameter>=<value>\r\n
[<parameter pair>]

<length> is the actual length of content.

**Example:** Request IP address and its response

Request:
http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress

Response:
HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: 33\r\n
\r\n
network.ipaddress=192.168.0.123\r\n

# 6. Set Server Parameter Values

**Note:** The access right depends on the URL directory.

**Method:** GET/POST

Syntax:

http://<*servername*>/cgi-bin/anonymous/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>][&return=<return page>]

http://<*servername*>/cgi-bin/viewer/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<*servername*>/cgi-bin/operator/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

http://<*servername*>/cgi-bin/admin/setparam.cgi? <*parameter*>=<*value*>
[&<parameter>=<value>…][&update=<value>] [&return=<return page>]

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| **<group>_<name>** | value to assigned | Assign <*value*> to the parameter <*group*>_<*name*>. |
| **update** | <boolean> | Set to 1 to update all fields (no need to update parameter in each group). |
| **return** | <*return page*> | Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page.<br><br>(Note: The return page can be a general HTML file (.htm, .html) or a VIVOTEK server script executable (.vspx) file. It cannot be a CGI command or have any extra parameters. This parameter must be placed at the end of the parameter list |

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/html\r\n
Context-Length: <length>\r\n
\r\n
<*parameter pair*>

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

Only the parameters that you set and are readable will be returned.

**Example:** Set the IP address of server to 192.168.0.123:

Request:

http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/html\r\n

Context-Length: 33\r\n

\r\n

network.ipaddress=192.168.0.123\r\n

# 7. Available parameters on the server

Valid values:

| VALID VALUES | DESCRIPTION |
|---|---|
| string[<n>] | Text strings shorter than 'n' characters. The characters ",', <,>,& are invalid. |
| string[n~m] | Text strings longer than `n' characters and shorter than `m' characters. The characters ",', <,>,& are invalid. |
| password[<n>] | The same as string but displays '*' instead. |
| integer | Any number between $(-2^{31} - 1)$ and $(2^{31} - 1)$. |
| positive integer | Any number between 0 and $(2^{32} - 1)$. |
| <m> ~ <n> | Any number between 'm' and 'n'. |
| domain name[<n>] | A string limited to a domain name shorter than 'n' characters (eg. www.ibm.com). |
| email address [<n>] | A string limited to an email address shorter than 'n' characters (eg. joe@www.ibm.com). |
| ip address | A string limited to an IP address (eg. 192.168.1.1). |
| mac address | A string limited to contain a MAC address without hyphens or colons. |
| boolean | A boolean value of 1 or 0 represents [Yes or No], [True or False], [Enable or Disable]. |
| <value1>,<br><value2>,<br><value3>,<br>... | Enumeration. Only given values are valid. |
| blank | A blank string. |
| everything inside <> | A description |

| | |
|---|---|
| integer primary key | SQLite data type. A 32-bit signed integer. The value is assigned a unique integer by the server. |
| text | SQLite data type. The value is a text string, stored using the database encoding (UTF-8, UTF-16BE or UTF-16-LE). |
| coordinate | x, y coordinate (eg. 0,0) |
| window size | window width and height (eg. 800x600) |

NOTE: The camera should not be restarted when parameters are changed.

# 7.1 system

Group: **system**

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| hostname | string[64] | Mega-Pixel Network Camera | 1/6 | Host name of server (Network Camera, Wireless Network Camera, Video Server, Wireless Video Server). |
| ledoff | <boolean> | 0 | 6/6 | Turn on (0) or turn off (1) all led indicators. |
| lowlight | <boolean> | 1 | 6/6 | Turn on white light LED under all conditions.<br>Only turn on white light LED in low light conditions.<br>(product dependent) |
| date | <YYYY/MM/DD>,<br>keep,<br>auto | <current date> | 6/6 | Current date of system. Set to 'keep' to keep date unchanged. Set to 'auto' to use NTP to synchronize date. |
| time | <hh:mm:ss>,<br>keep,<br>auto | <current time> | 6/6 | Current time of the system. Set to 'keep' to keep time unchanged. Set to 'auto' to use NTP to synchronize time. |
| datetime | <MMDDhhmmYYYY.ss> | <blank> | 6/6 | Another current time format of the system. |
| ntp | <domain | <blank> | 6/6 | NTP server. |

| | | | | |
|---|---|---|---|---|
| | name>,<br><ip address>,<br><blank> | | | *Do not use "skip to invoke default server" for default value. |
| timezoneindex | -489 ~ 529 | 320 | 6/6 | Indicate timezone and area.<br>-480: GMT-12:00 Eniwetok, Kwajalein<br>-440: GMT-11:00 Midway Island, Samoa<br>-400: GMT-10:00 Hawaii<br>-360: GMT-09:00 Alaska<br>-320: GMT-08:00 Las Vegas, San_Francisco, Vancouver<br>-280: GMT-07:00 Mountain Time, Denver<br>-281: GMT-07:00 Arizona<br>-240: GMT-06:00 Central America, Central Time, Mexico City, Saskatchewan<br>-200: GMT-05:00 Eastern Time, New York, Toronto<br>-201: GMT-05:00 Bogota, Lima, Quito, Indiana<br>-180: GMT-04:30 Caracas<br>-160: GMT-04:00 Atlantic Time, Canada, La Paz, Santiago<br>-140: GMT-03:30 Newfoundland<br>-120: GMT-03:00 Brasilia, Buenos Aires, Georgetown, Greenland<br>-80: GMT-02:00 Mid-Atlantic<br>-40: GMT-01:00 Azores, Cape_Verde_IS.<br>0: GMT Casablanca, Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London<br>40: GMT 01:00 Amsterdam, Berlin, Rome, Stockholm, Vienna, Madrid, Paris |

| | | | | |
|---|---|---|---|---|
| | | | | 41: GMT 01:00 Warsaw, Budapest, Bern<br>80: GMT 02:00 Athens, Helsinki, Istanbul, Riga<br>81: GMT 02:00 Cairo<br>82: GMT 02:00 Lebanon, Minsk<br>83: GMT 02:00 Israel<br>120: GMT 03:00 Baghdad, Kuwait, Riyadh, Moscow, St. Petersburg, Nairobi<br>121: GMT 03:00 Iraq<br>140: GMT 03:30 Tehran<br>160: GMT 04:00 Abu Dhabi, Muscat, Baku,<br>Tbilisi, Yerevan<br>180: GMT 04:30 Kabul<br>200: GMT 05:00 Ekaterinburg, Islamabad, Karachi, Tashkent<br>220: GMT 05:30 Calcutta, Chennai, Mumbai, New Delhi<br>230: GMT 05:45 Kathmandu<br>240: GMT 06:00 Almaty, Novosibirsk, Astana, Dhaka, Sri Jayawardenepura<br>260: GMT 06:30 Rangoon<br>280: GMT 07:00 Bangkok, Hanoi, Jakarta, Krasnoyarsk<br>320: GMT 08:00 Beijing, Chongging, Hong Kong, Kuala Lumpur, Singapore, Taipei<br>360: GMT 09:00 Osaka, Sapporo, Tokyo, Seoul, Yakutsk<br>380: GMT 09:30 Adelaide, Darwin<br>400: GMT 10:00 Brisbane, Canberra, Melbourne, Sydney, Guam, Vladivostok<br>440: GMT 11:00 Magadan, Solomon Is., New Caledonia<br>480: GMT 12:00 Aucklan, Wellington, Fiji, Kamchatka, |

| | | | | |
|---|---|---|---|---|
| | | | | Marshall Is.<br>520: GMT 13:00 Nuku'Alofa |
| daylight_enable | <boolean> | 0 | 6/6 | Enable automatic daylight saving time in time zone. |
| daylight_dstactualmode | <boolean> | 1 | 6/7 | Check if current time is under daylight saving time.<br>(Used internally) |
| daylight_auto_begintime | string[19] | NONE | 6/7 | Display the current daylight saving start time. |
| daylight_auto_endtime | string[19] | NONE | 6/7 | Display the current daylight saving end time. |
| daylight_timezones | string | ,-360,-320,-280,-240,-241,-200,-201,-160,-140,-120,-80,-40,0,40,41,80,81,82,83,120,140,380,400,480 | 6/6 | List time zone index which support daylight saving time. |
| updateinterval | 0,<br>3600,<br>86400,<br>604800,<br>2592000 | 0 | 6/6 | 0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals. |
| restore | 0,<br><positive integer> | N/A | 7/6 | Restore the system parameters to default values after <value> seconds. |
| reset | 0,<br><positive integer> | N/A | 7/6 | Restart the server after <value> seconds if <value> is non-negative. |
| restoreexceptnet | <Any value> | N/A | 7/6 | Restore the system parameters to default values except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will |

| | | | | |
|---|---|---|---|---|
| | | | | be restored to the default value except for a union of the combined results. |
| restoreexceptdst | <Any value> | N/A | 7/6 | Restore the system parameters to default values except all daylight saving time settings.<br>This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to default values except for a union of combined results. |
| restoreexceptlang | <Any Value> | N/A | 7/6 | Restore the system parameters to default values except the custom language file the user has uploaded.<br>This command can cooperate with other "restoreexceptXYZ" commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results. |

## 7.1.1 system.info

Subgroup of **system**: **info** (The fields in this group are unchangeable.)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| modelname | string[40] | FE8171 | 0/7 | Internal model name of the server (eg. IP7139) |
| extendedmodelname | string[40] | FE8171 | 0/7 | ODM specific model name of server (eg. DCS-5610). If it is not an ODM model, this field will be equal to "modelname" |
| serialnumber | <mac address> | <product mac address> | 0/7 | 12 characters MAC address (without hyphens). |
| firmwareversion | string[40] | <product dependent | 0/7 | Firmware version, including model, company, and |

| | | | | |
|---|---|---|---|---|
| | | > | | version number in the format: <MODEL-BRAND-VERSION> |
| language_count | <integer> | 9 | 0/7 | Number of webpage languages available on the server. |
| language_i<0~(count-1)> | string[16] | <product dependent> | 0/7 | Available language lists. |
| customlanguage_maxcount | <integer> | 1 | 0/6 | Maximum number of custom languages supported on the server. |
| customlanguage_count | <integer> | 0 | 0/6 | Number of custom languages which have been uploaded to the server. |
| customlanguage_i<0~(maxcount-1)> | string | <blank> | 0/6 | Custom language name. |

# 7.2 status

Group: **status**

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| videoactualmodulation <product dependent> | ntsc, pal | 1 | 4/7 | The actual modulation type (videoin.type=0). |
| di_i<0~(ndi-1)> <product dependent> | <boolean> | 0 | 1/7 | 0 => Inactive, normal 1 => Active, triggered (capability.ndi > 0) |
| do_i<0~(ndo-1)> <product dependent> | <boolean> | 0 | 1/7 | 0 => Inactive, normal 1 => Active, triggered (capability.ndo > 0) |
| daynight <product dependent> | day, night | <product dependent> | 7/7 | Current status of day, night. |
| onlinenum_rtsp | integer | 0 | 6/7 | Current number of RTSP connections. |
| onlinenum_httppush | integer | 0 | 6/7 | Current number of HTTP push server connections. |
| eth_i0 | <string> | <product | 1/7 | Get network information |

| | | | | |
|---|---|---|---|---|
| | | dependent> | | from mii-tool. |
| vi_i<0~(nvi-1)><br><product dependent> | <boolean> | 0 | 1/7 | Virtual input<br>0 => Inactive<br>1 => Active<br>(capability.nvi > 0) |

# 7.3 digital input behavior define

Group: **di_i<0~(ndi-1)>** (capability.ndi > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| normalstate | high,<br>low | high | 1/1 | Indicates open circuit or closed circuit (inactive status) |

# 7.4 digital output behavior define

Group: **do_i<0~(ndo-1)>** (capability.ndo > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| normalstate | open,<br>grounded | open | 1/1 | Indicate open circuit or closed circuit (inactive status) |

# 7.5 security

Group: security

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| privilege_do<br><product dependent> | view, operator, admin | operator | 6/6 | Indicate which privileges and above can control digital output (capability.ndo > 0) |
| privilege_camctrl<br><product dependent> | view, operator, admin | view | 6/6 | Indicate which privileges and above can control PTZ (capability.ptzenabled > 0 or capability.eptz > 0) |
| user_i0_name | string[64] | root | 6/7 | User name of root |
| user_i<1~20>_name | string[64] | <blank> | 6/7 | User name |
| user_i0_pass | password[64] | <blank> | 6/6 | Root password |

| | | | | |
|---|---|---|---|---|
| user_i<1~20>_pass | password[64] | <blank> | 7/6 | User password |
| user_i0_privilege | viewer,<br>operator,<br>admin | admin | 6/7 | Root privilege |
| user_i<1~20>_ privilege | viewer,<br>operator,<br>admin | <blank> | 6/6 | User privilege |

# 7.6 network

Group: **network**

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| preprocess | <positive integer> | <blank> | 7/6 | An 32-bit integer, each bit can be set separately as follows:<br>Bit 0 => HTTP service;<br>Bit 1=> HTTPS service;<br>Bit 2=> FTP service;<br>Bit 3 => Two way audio and RTSP Streaming service;<br><br>To stop service before changing its port settings. It's **recommended** to set this parameter when change a service port to the port occupied by another service currently. Otherwise, the service may fail.<br>Stopped service will auto-start after changing port settings.<br>Ex:<br>Change HTTP port from 80 to 5556, and change RTP port for video from 5556 to 20480.<br>Then, set preprocess=9 to stop both service first.<br>"/cgi-bin/admin/setparam.cgi?<br>network_preprocess=9&network_http_port=5556& network_rtp_videoport=20480" |
| type | lan,<br>pppoe<br><product dependent> | lan | 6/6 | Network connection type. |
| resetip | <boolean> | 1 | 6/6 | 1 => Get ipaddress, subnet, router, dns1, dns2 |

| | | | | |
|---|---|---|---|---|
| | | | | from DHCP server at next reboot.<br>0 => Use preset ipaddress, subnet, rounter, dns1, and dns2. |
| ipaddress | <ip address> | <product dependent> | 6/6 | IP address of server. |
| subnet | <ip address> | <blank> | 6/6 | Subnet mask. |
| router | <ip address> | <blank> | 6/6 | Default gateway. |
| dns1 | <ip address> | <blank> | 6/6 | Primary DNS server. |
| dns2 | <ip address> | <blank> | 6/6 | Secondary DNS server. |
| wins1 | <ip address> | <blank> | 6/6 | Primary WINS server. |
| wins2 | <ip address> | <blank> | 6/6 | Secondary WINS server. |

## 7.6.1 802.1x

Subgroup of **network: ieee8021x** (capability.protocol.ieee8021x > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 6/6 | Enable/disable IEEE 802.1x |
| eapmethod | eap-peap, eap-tls | eap-peap | 6/6 | Selected EAP method |
| identity_peap | String[64] | <blank> | 6/6 | PEAP identity |
| identity_tls | String[64] | <blank> | 6/6 | TLS identity |
| password | String[254] | <blank> | 6/6 | Password for TLS |
| privatekeypassword | String[254] | <blank> | 6/6 | Password for PEAP |
| ca_exist | <boolean> | 0 | 6/6 | CA installed flag |
| ca_time | <integer> | 0 | 6/7 | CA installed time.<br>Represented in EPOCH |
| ca_size | <integer> | 0 | 6/7 | CA file size (in bytes) |
| certificate_exist | <boolean> | 0 | 6/6 | Certificate installed flag (for TLS) |
| certificate_time | <integer> | 0 | 6/7 | Certificate installed time.<br>Represented in EPOCH |
| certificate_size | <integer> | 0 | 6/7 | Certificate file size (in bytes) |

| | | | | |
|---|---|---|---|---|
| privatekey_exist | <boolean> | 0 | 6/6 | Private key installed flag (for TLS) |
| privatekey_time | <integer> | 0 | 6/7 | Private key installed time. Represented in EPOCH |
| privatekey_size | <integer> | 0 | 6/7 | Private key file size (in bytes) |

## 7.6.2 QOS

Subgroup of **network: qos_cos** (capability.protocol.qos.cos > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 6/6 | Enable/disable CoS (IEEE 802.1p) |
| vlanid | 1~4095 | 1 | 6/6 | VLAN ID |
| video | 0~7 | 0 | 6/6 | Video channel for CoS |
| audio <product dependent> | 0~7 | 0 | 6/6 | Audio channel for CoS (capability.naudio > 0) |
| eventalarm | 0~7 | 0 | 6/6 | Event/alarm channel for CoS |
| management | 0~7 | 0 | 6/6 | Management channel for CoS |
| eventtunnel | 0~7 | 0 | 6/6 | Event/Control channel for CoS |

Subgroup of **network: qos_dscp** (capability.protocol.qos.dscp > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 6/6 | Enable/disable DSCP |
| video | 0~63 | 0 | 6/6 | Video channel for DSCP |
| audio | 0~63 | 0 | 6/6 | Audio channel for DSCP (capability.naudio > 0) |
| eventalarm | 0~63 | 0 | 6/6 | Event/alarm channel for DSCP |
| management | 0~63 | 0 | 6/6 | Management channel for DSCP |
| eventtunnel | 0~63 | 0 | 6/6 | Event/Control channel for DSCP |

## 7.6.3 IPV6

Subgroup of **network**: **ipv6** (capability.protocol.ipv6 > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 6/6 | Enable IPv6. |
| addonipaddress | <ip address> | <blank> | 6/6 | IPv6 IP address. |
| addonprefixlen | 0~128 | 64 | 6/6 | IPv6 prefix length. |
| addonrouter | <ip address> | <blank> | 6/6 | IPv6 router address. |
| addondns | <ip address> | <blank> | 6/6 | IPv6 DNS address. |
| allowoptional | <boolean> | 0 | 6/6 | Allow manually setup of IP address setting. |

## 7.6.4 FTP

Subgroup of **network**: **ftp**

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| port | 21, 1025~65535 | 21 | 6/6 | Local ftp server port. |

## 7.6.5 HTTP

Subgroup of **network**: **http**

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| port | 80, 1025 ~ 65535 | 80 | 1/6 | HTTP port. |
| alternateport | 1025~65535 | 8080 | 6/6 | Alternate HTTP port. |
| authmode | basic, digest | basic | 1/6 | HTTP authentication mode. |
| s0_accessname | string[32] | video.mjpg | 1/6 | HTTP server push access name for stream 1. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 0) |
| s1_accessname <product dependent> | string[32] | video2.mjpg | 1/6 | HTTP server push access name for stream 2. (capability.protocol.spush_mjpeg |

| | | | | |
|---|---|---|---|---|
| | | | | =1 and capability.nmediastream > 1) |
| s2_accessname <product dependent> | string[32] | video3.mjpg | 1/6 | Http server push access name for stream 3 (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 2) |
| anonymousviewing | <boolean> | 0 | 1/6 | Enable anoymous streaming viewing. |

## 7.6.6 HTTPS port

Subgroup of **network**: **https_port** (capability.protocol.https > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| port | 443, 1025 ~ 65535 | 443 | 1/6 | HTTPS port. |

## 7.6.7 RTSP

Subgroup of **network**: **rtsp** (capability.protocol.rtsp > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| port | 554, 1025 ~ 65535 | 554 | 1/6 | RTSP port. (capability.protocol.rtsp=1) |
| anonymousviewing | <boolean> | 0 | 1/6 | Enable anoymous streaming viewing. |
| authmode | disable, basic, digest | disable | 1/6 | RTSP authentication mode. (capability.protocol.rtsp=1) |
| s0_accessname | <boolean> | live.sdp | 1/6 | RTSP access name for stream1. (capability.protocol.rtsp=1 and capability.nmediastream > 0) |
| s1_accessname | <boolean> | live2.sdp | 1/6 | RTSP access name for stream2. (capability.protocol.rtsp=1 and capability.nmediastream > 1) |

| | | | | |
|---|---|---|---|---|
| s2_accessname | <boolean> | live3.sdp | 1/6 | RTSP access name for stream3 (capability.protocol.rtsp=1 and capability.nmediastream > 2) |

# 7.6.7.1 RTSP multicast

Subgroup of **network_rtsp_s<0~(n-1)>**: **multicast,** n is stream count (capability.protocol.rtp.multicast > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| alwaysmulticast | <boolean> | 0 | 4/4 | Enable always multicast. |
| ipaddress | <ip address> | For n=0, 239.128.1.99 For n=1, 239.128.1.100, and so on. | 4/4 | Multicast IP address. |
| videoport | 1025 ~ 65535 | 5562+n*2 <product dependent> | 4/4 | Multicast video port. |
| audioport <product dependent> | 1025 ~ 65535 | 5564+n*2 <product dependent> | 4/4 | Multicast audio port. (capability.naudio > 0) |
| ttl | 1 ~ 255 | 15 | 4/4 | Mutlicast time to live value. |

## 7.6.8 SIP port

Subgroup of **network**: **sip** (capability.protocol.sip> 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| port | 1025 ~ 65535 | 5060 | 1/6 | SIP port. |

## 7.6.9 RTP port

Subgroup of **network**: **rtp**

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| videoport | 1025 ~ 65535 | 5556 | 6/6 | Video channel port for RTP. |

| | | | | |
|---|---|---|---|---|
| | | | | (capability.protocol.rtp_unicast=1) |
| audioport | 1025 ~ 65535 | 5558 | 6/6 | Audio channel port for RTP. (capability.protocol.rtp_unicast=1) |

## 7.6.10 PPPoE

Subgroup of **network**: **pppoe** (capability.protocol.pppoe > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| user | string[128] | <blank> | 6/6 | PPPoE account user name. |
| pass | password[64] | <blank> | 6/6 | PPPoE account password. |

# 7.7 IP Filter

Group: ipfilter

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 6/6 | Enable access list filtering. |
| admin_enable | <boolean> | 0 | 6/6 | Enable administrator IP address. |
| admin_ip | String[44] | <blank> | 6/6 | Administrator IP address. |
| maxconnection | 1~10 | 10 | 6/6 | Maximum number of concurrent streaming connection(s). |
| type | 0, 1 | 1 | 6/6 | Ipfilter policy :<br>0 => allow<br>1 => deny |
| ipv4list_i<0~9> | Single address: <ip address><br>Network address: <ip address / network mask><br>Range address:<start ip address - end ip address> | <blank> | 6/6 | IPv4 address list. |
| ipv6list_i<0~9> | String[44] | <blank> | 6/6 | IPv6 address list. |

# 7.8 Video input

Group: **videoin**

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| cmosfreq | 50, 60 | 60 | 4/4 | CMOS frequency. (capability.videoin.type=2) |
| whitebalance | auto, manual | auto | 4/4 | "auto" indicates auto white balance.<br>"manual" indicates keep current value. |
| exposurelevel | 0~12 | 6 | 4/4 | Exposure level |
| enableblc | <boolean> | 0 | 4/4 | Enable backlight compensation. |
| color | 0, 1 | 1 | 4/4 | 0 =>monochrome<br>1 => color |
| flip | <boolean> | 0 | 4/4 | Flip the image. |
| mirror | <boolean> | 0 | 4/4 | Mirror the image. |
| ptzstatus | <integer> | 2 | 1/7 | A 32-bit integer, each bit can be set separately as follows:<br>Bit 0 => Support camera control function; 0(not support), 1(support)<br>Bit 1 => **Built-in** or **external** camera; 0 (external), 1(built-in)<br>Bit 2 => Support **pan** operation; 0(not support), 1(support)<br>Bit 3 => Support **tilt** operation; 0(not support), 1(support)<br>Bit 4 => Support **zoom** operation; 0(not support), 1(support)<br>Bit 5 => Support **focus** operation; 0(not support), 1(support) |
| text | string[16] | <blank> | 1/4 | Enclose caption. |
| imprinttimestamp | <boolean> | 0 | 4/4 | Overlay time stamp on video. |

| | | | | |
|---|---|---|---|---|
| maxexposure | 1, 15, 30, 60, 120, 240, 480 <product dependent> | 30 | 4/4 | Maximum exposure time. |
| options | framerate | framerate | 4/4 | Video input option:<br>(1) video frame rate first mode |
| enablepreview | <boolean> | 0 | 1/4 | Usage for UI of exposure settings. Preview settings of video profile. |

## 7.8.1 Video input setting per channel

Group: **videoin_c<0~(n-1)>** for n channel products, and m is stream number

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| cmosfreq | 50, 60 | 60 | 4/4 | CMOS frequency.<br>(capability.videoin.type=2) |
| whitebalance | auto, manual | auto | 4/4 | "auto" indicates auto white balance.<br>"manual" indicates keep current value. |
| rgain | 0~100 | 30 | 4/4 | Manual set rgain value of gain control setting. |
| bgain | 0~100 | 30 | 4/4 | Manual set bgain value of gain control setting. |
| exposurelevel | 0~12 | 6 | 4/4 | Exposure level |
| enableblc | 0~1 | 0 | 4/4 | Enable backlight compensation |
| agcmode | auto,fixed | 1 | 4/4 | Set auto gain control mode. |
| maxgain | 0~100 | 100 | 4/4 | Manual set maximum gain value. |
| mingain | 0~100 | 0 | 4/4 | Manual set minimum gain value. |
| color | 0, 1 | 1 | 4/4 | 0 =>monochrome<br>1 => color |
| flip | <boolean> | 0 | 4/4 | Flip the image. |
| mirror | <boolean> | 0 | 4/4 | Mirror the image. |
| ptzstatus | <integer> | 2 | 1/7 | A 32-bit integer, each bit can |

| | | | | |
|---|---|---|---|---|
| | | | | be set separately as follows:<br>Bit 0 => Support camera control function; 0(not support), 1(support)<br>Bit 1 => **Built-in** or **external** camera; 0 (external), 1(built-in)<br>Bit 2 => Support **pan** operation; 0(not support), 1(support)<br>Bit 3 => Support **tilt** operation; 0(not support), 1(support)<br>Bit 4 => Support **zoom** operation; 0(not support), 1(support)<br>Bit 5 => Support **focus** operation; 0(not support), 1(support) |
| text | string[60] | <blank> | 1/4 | Enclose caption. |
| imprinttimestamp | <boolean> | 0 | 4/4 | Overlay time stamp on video. |
| exposuremode | auto,fixed | auto | 4/4 | Exposure mode |
| flickerless | <boolean> | 0 | 4/4 | Avoid flickering on images. |
| minexposure | 1~32000 | 32000 | 4/4 | Minimum exposure time. |
| maxexposure | 1~32000 | 30 | 4/4 | Maximum exposure time. |
| options | crop | crop | 4/4 | Video input option: cropping mode |
| crop_size | <window size> (WxH) | 1952x1944 | 1/4 | Crop width and height.<br>(1)1952x1944<br>(2)1920x1080 |
| enablepreview | <boolean> | 0 | 1/4 | Usage for UI of exposure settings. Preview settings of video profile. |
| s<0~(m-1)>_codectype | mpeg4, mjpeg, h264, svc | H264 | 1/4 | Video codec type.<br>svc is only supported with stream 0. |
| s<0~(m-1)>_resolution | Reference capability_videoin_resolution | 1536x1536 | 1/4 | Video resolution in pixels. |

| | | | | |
|---|---|---|---|---|
| s<0~(m-1)>_mpeg4_intraperiod | 250, 500, 1000, 2000, 3000, 4000 | 1000 | 4/4 | Intra frame period in milliseconds. |
| s<0~(m-1)>_mpeg4_bitraterestriction | average, upperbound | average | 4/4 | "average" indicates the average bit rate will be equal to its target bit rate.<br>"upperbound" indicates the bit rate will always not exceed its target bit rate. |
| s<0~(m-1)>_mpeg4_prioritypolicy | framerate, imagequality | framerate | 4/4 | The policy to apply when the target bit rate is not sufficient to satisfy current encoded conditions.<br>"framerate" indicates frame rate first.<br>"imagequality" indicates image quality first. |
| s<0~(m-1)>_mpeg4_ratecontrolmode | cbr, vbr | vbr | 4/4 | cbr, constant bitrate<br>vbr, fix quality |
| s<0~(m-1)>_mpeg4_quant | 1~5<br>99, 100 | 3 | 4/4 | Quality of video when choosing vbr in "ratecontrolmode".<br>99 is the customized manual input setting.<br>1 = worst quality, 5 = best quality.<br>100 is percentage mode. |
| s<0~(m-1)>_mpeg4_qvalue | 2~31 | 7 | 4/4 | Manual video quality level input.<br>(s<0~(m-1)>_mpeg4_quant = 99) |
| s<0~(m-1)>_mpeg4_qpercent | 1~100 | 29 | 4/4 | Manual video quality level input.<br>(s<0~(m-1)>_mpeg4_quant = 100) |
| s<0~(m-1)>_mpeg4_bitrate | 1000~16000000<br><product dependent> | 3000000 | 4/4 | Set bit rate in bps when choosing cbr in "ratecontrolmode". |
| s<0~(m-1)>_mpeg4_maxfr | 1~15 | 15 | 1/4 | Set maximum frame rate in |

| | | | | |
|---|---|---|---|---|
| ame | | | | fps (for MPEG-4). |
| s<0~(m-1)>_svc_intraperiod | 250, 500, 1000, 2000, 3000, 4000 | 1000 | 4/4 | Intra frame period in milliseconds. |
| s<0~(m-1)>_svc_svclayer | 3 | 3 | 1/4 | SVC temporal layer. |
| s<0~(m-1)>_svc_svcsyntax | 0~1 | 0 | 1/4 | Enable SVC syntax or not. |
| s<0~(m-1)>_svc_bitraterestriction | average, upperbound | average | 4/4 | "average" indicates the average bit rate will be equal to its target bit rate.<br>"upperbound" indicates the bit rate will always not exceed its target bit rate. |
| s<0~(m-1)>_svc_prioritypolicy | framerate, imagequality | framerate | 4/4 | The policy to apply when the target bit rate is not sufficient to satisfy current encoded conditions.<br>"framerate" indicates frame rate first.<br>"imagequality" indicates image quality first. |
| s<0~(m-1)>_svc_ratecontrolmode | cbr, vbr | vbr | 4/4 | cbr, constant bitrate<br>vbr, fix quality |
| s<0~(m-1)>_svc_quant | 1~5<br>99, 100 | 3 | 4/4 | Quality of video when choosing vbr in "ratecontrolmode".<br>99 is the customized manual input setting.<br>1 = worst quality, 5 = best quality.<br>100 is percentage mode. |
| s<0~(m-1)>_svc_qvalue | 0~51 | 2 | 4/4 | Manual video quality level input.<br>(s<0~(m-1)>_svc_quant = 99) |
| s<0~(m-1)>_svc_qpercent | 1~100 | 44 | 4/4 | Manual video quality level input.<br>(s<0~(m-1)>_svc_quant = 100) |
| s<0~(m-1)>_svc_bitrate | 1000~16000000 | 30000000 | 4/4 | Set bit rate in bps when choosing cbr in |

| | | | | |
|---|---|---|---|---|
| | | | | "ratecontrolmode". |
| s<0~(m-1)>_svc_maxframe | 1~25,<br>26~30 (only for NTSC or 60Hz CMOS) | 30 | 1/4 | Set maximum frame rate in fps (for svc). |
| s<0~(m-1)>_svc_profile | 0~2 | 1 | 1/4 | Indicate SVC profiles<br>0: baseline<br>1: main profile<br>2: high profile |
| s<0~(m-1)>_h264_intraperiod | 250, 500, 1000, 2000, 3000, 4000 | 1000 | 4/4 | Intra frame period in milliseconds. |
| s<0~(m-1)>_h264_bitraterestriction | average, upperbound | average | 4/4 | "average" indicates the average bit rate will be equal to its target bit rate.<br>"upperbound" indicates the bit rate will always not exceed its target bit rate. |
| s<0~(m-1)>_h264_prioritypolicy | framerate, imagequality | framerate | 4/4 | The policy to apply when the target bit rate is not sufficient to satisfy current encoded conditions.<br>"framerate" indicates frame rate first.<br>"imagequality" indicates image quality first. |
| s<0~(m-1)>_h264_ratecontrolmode | cbr, vbr | vbr | 4/4 | cbr, constant bitrate<br>vbr, fix quality |
| s<0~(m-1)>_h264_quant | 1~5<br>99, 100 | 3 | 4/4 | Quality of video when choosing vbr in "ratecontrolmode".<br>99 is the customized manual input setting.<br>1 = worst quality, 5 = best quality.<br>100 is percentage mode. |
| s<0~(m-1)>_h264_qvalue | 0~51 | 2 | 4/4 | Manual video quality level input.<br>(s<0~(m-1)>_h264_quant = 99) |

| | | | | |
|---|---|---|---|---|
| s<0~(m-1)>_h264_qpercent | 1~100 | 44 | 4/4 | Manual video quality level input.<br>(s<0~(m-1)>_h264_quant = 100) |
| s<0~(m-1)>_h264_bitrate | 1000~16000000 | 3000000 | 4/4 | Set bit rate in bps when choosing cbr in "ratecontrolmode". |
| s<0~(m-1)>_h264_maxframe | 1~15 | 15 | 1/4 | Set maximum frame rate in fps (for h264). |
| s<0~(m-1)>_h264_profile <product dependent> | 0~2 | 1 | 1/4 | Indicate H264 profiles<br>0: baseline<br>1: main profile<br>2: high profile |
| s<0~(m-1)>_mjpeg_bitraterestriction | average, upperbound | average | 4/4 | "average" indicates the average bit rate will be equal to its target bit rate.<br>"upperbound" indicates the bit rate will always not exceed its target bit rate. |
| s<0~(m-1)>_mjpeg_prioritypolicy | framerate, imagequality | framerate | 4/4 | The policy to apply when the target bit rate is not sufficient to satisfy current encoded conditions.<br>"framerate" indicates frame rate first.<br>"imagequality" indicates image quality first. |
| s<0~(m-1)>_mjpeg_ratecontrolmode | cbr, vbr | vbr | 4/4 | cbr, constant bitrate<br>vbr, fix quality |
| s<0~(m-1)>_mjpeg_quant | 1~5<br>99, 100 | 3 | 4/4 | Quality of JPEG video.<br>99 is the customized manual input setting.<br>1 = worst quality, 5 = best quality.<br>100 is percentage mode. |
| s<0~(m-1)>_mjpeg_qvalue | 2~97 | 50 | 4/4 | Manual video quality level input.<br>(s<0~(m-1)>_mjpeg_quant = 99) |
| s<0~(m-1)>_mjpeg_qperce | 1~100 | 49 | 4/4 | Manual video quality level |

| | | | | |
|---|---|---|---|---|
| nt | | | | input.<br>(s<0~(m-1)>_mjpeg_quant = 100) |
| s<0~(m-1)>_mjpeg_maxframe | 1~15 | 15 | 1/4 | Set maximum frame rate in fps (for JPEG). |
| s<0~(m-1)>_mjpeg_bitrate | 1000~16000000 | 30000000 | 4/4 | Set bit rate in bps when choosing cbr in "ratecontrolmode". |
| s<0~(m-1)>_forcei | 1 | N/A | 7/6 | Force I frame. |
| wdrc_mode | 0~2 | 0 | 4/4 | WDR enhanced.<br>0: off<br>1: Sensitivity low<br>2: Sensitivity high |
| wdrc_strength | 0~2 | 1 | 4/4 | WDR enhanced.<br>0: low<br>1: medium<br>2: high |
| mounttype | ceiling, wall, floor | wall | 1/6 | Mount type |
| enableimgreport | 0, 1 | 0 | 1/6 | Image report |
| enablewatermark | 0, 1 | 0 | 1/6 | Watermark |

# 7.8.1.1 Alternative video input profiles per channel

In addition to the primary setting of video input, there can be alternative profile video input setting for each channel which might be for different scene of light (daytime or nighttime).

Group: **videoin_c0_profile_i<0~(m-1)>** (capability. nvideoinprofile > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 4/4 | Enable/disable this profile setting |
| policy | day,<br>night,<br>schedule | night | 4/4 | The mode which the profile is applied to. |
| begintime | hh:mm | 18:00 | 4/4 | Begin time of schedule mode. |
| endtime | hh:mm | 06:00 | 4/4 | End time of schedule mode. |
| exposuremode | auto,fixed | auto | 4/4 | Exposure Mode |
| flickerless | <boolean> | 0 | 4/4 | Avoid flickering on images. |
| minexposure | 1~32000 | 32000 | 4/4 | Minimum exposure time. |

| | | | | |
|---|---|---|---|---|
| maxexposure | 1~32000 | 30 | 4/4 | Maximum exposure time. |
| enableblc | <boolean> | 0 | 4/4 | Enable backlight compensation. |
| exposurelevel | 0~12 | 6 | 4/4 | Exposure level |
| agcmode | auto,fixed | auto | 4/4 | Set auto gain control mode. |
| maxgain | 0~100 | 100 | 4/4 | Manual set maximum gain value. |
| mingain | 0~100 | 0 | 4/4 | Manual set minimum gain value. |
| whitebalance | auto, manual | auto | 4/4 | "auto" indicates auto white balance.<br>"manual" indicates keep current value. |
| rgain | 0~100 | 30 | 4/4 | Manual set rgain value of gain control setting. |
| bgain | 0~100 | 30 | 4/4 | Manual set bgain value of gain control setting. |
| wdrc_mode | 0~2 | 0 | 4/4 | WDR enhanced.<br>0: off<br>1: Sensitivity low<br>2: Sensitivity high |
| wdrc_strength | 0~2 | 1 | 4/4 | WDR enhanced.<br>0: low<br>1: medium<br>2: high |

# 7.9 Video input preview

The temporary settings for video preview

Group: videoinpreview

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| exposuremode | auto,fixed | auto | 4/4 | Exposure Mode |
| minexposure | 1~32000 | 32000 | 4/4 | Minimum exposure time. |
| maxexposure | 1~32000 | 30 | 4/4 | Maximum exposure time. |
| exposurelevel | 0~12 | 6 | 4/4 | Exposure level |
| enableblc | <boolean> | 0 | 4/4 | Enable backlight compensation. |
| wdrc_mode | 0~2 | 0 | 4/4 | WDR enhanced.<br>0: off<br>1: Sensitivity low<br>2: Sensitivity high |
| wdrc_strength | 0~2 | 1 | 4/4 | WDR enhanced. |

| | | | | |
|---|---|---|---|---|
| | | | | 0: low<br>1: medium<br>2: high |
| agcmode | auto,fixed | auto | 4/4 | Set auto gain control mode. |
| maxgain | 0~100 | 100 | 4/4 | Manual set maximum gain value. |
| mingain | 0~100 | 0 | 4/4 | Manual set minimum gain value. |

# 7.10 IR cut control

Group: **ircutcontrol** (capability.nvideoinprofile > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| mode | auto,<br>day,<br>night,<br>di,<br>schedule<br><product dependent> | auto | 6/6 | Set IR cut control mode |
| daymodebegintime | 00:00~23:59 | 07:00 | 6/6 | Day mode begin time |
| daymodeendtime | 00:00~23:59 | 18:00 | 6/6 | Day mod end time |
| bwmode | <boolean> | 1 | 6/6 | Switch to B/W in night mode if enabled |
| sensitivity | low,<br>normal,<br>high | normal | 6/6 | Sensitivity of light sensor |
| enableextled | <boolean> | 0 | 1/6 | External IR led enable |

# 7.11 Image setting per channel

Group: **image_c<0~(n-1)>** for n channel products

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| brightness | -5~5 | -5 | 4/4 | Adjust brightness of image according to mode settings. |
| saturation | -5~5,100 | 0 | 4/4 | Adjust saturation of image according to mode settings. 100 for saturation percentage mode. |
| saturationpercent | 0~100 | 50 | 4/4 | Adjust saturation value of percentage when saturation=100 |
| contrast | -5 ~ 5 | 0 | 4/4 | Adjust contrast of image according to mode settings. |
| sharpness | -3~3,100 | 0 | 4/4 | Adjust sharpness of image according to mode settings. |
| sharpnesspercent | 0~100 | 50 | 4/4 | Adjust sharpness value of percentage when sharpness=100 |
| gammacurve | 0~100 | 0 | 4/4 | Gamma curve. |
| lowlightmode | <boolean> | 1 | 4/4 | Enable/disable low light mode. |
| profile_i0_enable | <boolean> | 0 | 4/4 | Enable/disable this profile setting |
| profile_i0_policy | day, night, schedule | night | 4/4 | The mode which the profile is applied to. |
| profile_i0_begintime | hh:mm | 18:00 | 4/4 | Begin time of schedule mode. |
| profile_i0_endtime | hh:mm | 06:00 | 4/4 | End time of schedule mode. |
| profile_i0_brightness | -5~5 | -5 | 4/4 | Adjust brightness of image according to mode settings. |
| profile_i0_saturation | -5~5,100 | 0 | 4/4 | Adjust saturation of image according to mode settings. 100 for saturation percentage mode. |
| profile_i0_saturationpercent | 0~100 | 50 | 4/4 | Adjust saturation value of percentage when saturation=100 |
| profile_i0_contrast | -5 ~ 5 | 0 | 4/4 | Adjust contrast of image according to mode settings. |
| profile_i0_sharpness | -3~3 | 0 | 4/4 | Adjust sharpness of image |

| | | | | |
|---|---|---|---|---|
| | | | | according to mode settings. |
| profile_i0_sharpnesspercent | 0~100 | 50 | 4/4 | Adjust sharpness value of percentage when sharpness=100 |
| profile_i0_gammacurve | 0~100 | 0 | 4/4 | Gamma curve |
| profile_i0_lowlightmode | <boolean> | 1 | 4/4 | Enable/disable low light mode. |
| profile_i0_wdrcstrength | 0~2 | 1 | 4/4 | WDR enhanced<br>0: low<br>1: medium<br>2: high |
| profile_i0_wdrcmode | 0~2 | 0 | 4/4 | WDR enhanced<br>0: off<br>1: Sensitivity low<br>2: Sensitivity high |

# 7.12 Image setting for preview

Group: **imagepreview_c<0~(n-1)>** for n channel products

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| brightness | -5~5 | -5 | 4/4 | Adjust brightness of image according to mode settings. |
| saturation | -5~5,100 | 0 | 4/4 | Adjust saturation of image according to mode settings. 100 for saturation percentage mode. |
| saturationpercent | 0~100 | 50 | 4/4 | Adjust saturation value of percentage when saturation=100 |
| contrast | -5 ~ 5 | 0 | 4/4 | Adjust contrast of image according to mode settings. |
| sharpness | -3~3,100 | 0 | 4/4 | Adjust sharpness of image according to mode settings. |
| sharpnesspercent | 0~100 | 50 | 4/4 | Adjust sharpness value of percentage when sharpness=100 |
| gammacurve | 0~100 | 0 | 4/4 | Gamma curve |
| lowlightmode | <boolean> | 0 | 4/4 | Enable/disable low light mode. |

Group: imagepreview

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| videoin_whitebalance | auto, manual | auto | 4/4 | Preview of adjusting white balance of image according to mode settings |
| videoin_restoreatwb | 0, 1~ | 0 | 4/4 | Restore of adjusting white balance of image according to mode settings |
| videoin_rgain | 0~100 | 0 | 4/4 | Manual set rgain value of gain control setting. |
| videoin_bgain | 0~100 | 0 | 4/4 | Manual set bgain value of gain control setting. |

# 7.13 Exposure window setting per channel

Group: **exposurewin_c<0~(n-1)>** for n channel products

(capability_videoin_supportexpwin = 1)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| mode | auto, custom, blc | auto | 4/4 | The mode indicates how to decide the exposure.<br>auto: Use full view as the only one exposure window.<br>custom: Use inclusive and exclusive window.<br>blc: Use BLC. |
| win_i<0~9>_enable | <boolean> | 0 | 4/4 | Enable or disable the window. |
| win_i<0~9>_policy | 0~1 | 0 | 4/4 | 0: Indicate exclusive.<br>1: Indicate inclusive. |
| win_i<0~9>_home | <coordinate> | (150,110) | 4/4 | Left-top corner coordinate of the window. |
| win_i<0~9>_size | <window size> | (100x75) | 4/4 | Width and height of the window. |

Group: **exposurewin_c<0~(n-1)>_profile** for m profile and n channel product

(capability_videoin_supportexpwin = 1)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| i<0~(m-1)>_mode | auto, custom, blc | auto | 4/4 | The mode indicates how to decide the exposure.<br>auto: Use full view as the only one exposure window.<br>custom: Use inclusive and |

| | | | | |
|---|---|---|---|---|
| | | | | exclusive window.<br>blc: Use BLC. |
| i<0~(m-1)>_win_i<0~9>_enable | <boolean> | 0 | 4/4 | Enable or disable the window. |
| i<0~(m-1)>_win_i<0~9>_policy | 0~1 | 0 | 4/4 | 0: Indicate exclusive.<br>1: Indicate inclusive. |
| i<0~(m-1)>_win_i<0~9>_home | <coordinate> | (150,110) | 4/4 | Left-top corner coordinate of the window. |
| i<0~(m-1)>_win_i<0~9>_size | <window size> | (100x75) | 4/4 | Width and height of the window. |

# 7.14 Audio input per channel

Group: **audioin_c<0~(n-1)>** for n channel products (capability.naudioin>0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| source | micin,<br>linein | micin | 4/4 | micin => use built-in microphone input.<br>linein => use external microphone input. |
| mute | 0, 1 | 0 | 4/4 | Enable audio mute. |
| gain | 1~100 | 65 | 4/4 | Gain of input.<br>(audioin_c<0~(n-1)>_source = linein) |
| boostmic | 1~100 | 65 | 4/4 | Enable microphone boost.<br>0 => +0dB<br>1 => +20dB<br>2 => +40dB<br>Or<br>Gain of input.<br>(audioin_c<0~(n-1)>_source = micin) |
| s<0~(m-1)>_codectype | aac4, gamr, g711 | aac4 | 4/4 | Set audio codec type for input. |
| s<0~(m-1)>_aac4_bitrate <product dependent> | 16000,<br>32000,<br>48000,<br>64000,<br>96000,<br>128000 | 16000 | 4/4 | Set AAC4 bitrate in bps. |

| | | | | |
|---|---|---|---|---|
| s<0~(m-1)>_gamr_bitrate <product dependent> | 4750, 5150, 5900, 6700, 7400, 7950, 10200, 12200 | 12200 | 4/4 | Set AMR bitrate in bps. |
| s<0~(m-1)>_g711_mode <product dependent> | pcmu, pcma | pcmu | 4/4 | Set G.711 mode. |

# 7.15 Time Shift settings

Group: **timeshift**, c for n channel products, m is stream number

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 4/4 | Enable time shift streaming. |
| c<0~(n-1)>_s<0~(m-1)>_allow | <boolean> | 0 | 4/4 | Enable time shift streaming for specific stream. |

# 7.16 Motion detection settings

Group: **motion_c<0~(n-1)>** for n channel product

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 4/4 | Enable motion detection. |
| win_i<0~4>_enable | <boolean> | 0 | 4/4 | Enable motion window 1~3. |
| win_i<0~4>_name | string[14] | <blank> | 4/4 | Name of motion window 1~3. |
| win_i<0~4>_polygon | 0 ~ 320,0 ~ 240, 0 ~ 320,0 ~ 240, 0 ~ 320,0 ~ 240, 0 ~ 320,0 ~ 240 | 0 | 4/4 | Coordinate of polygon window position. (4 points: x0,y0,x1,y1,x2,y2,x3,y3) |
| win_i<0~4>_objsize | 0 ~ 100 | 0 | 4/4 | Percent of motion detection window. |
| win_i<0~4>_sensitivity | 0 ~ 100 | 0 | 4/4 | Sensitivity of motion detection window. |

Group: **motion_c<0~(n-1)>_profile** for m profile and n channel product (capability.nmotionprofile > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| i<0~(m-1)>_enable | <boolean> | 0 | 4/4 | Enable profile 1 ~ (m-1). |
| i<0~(m-1)>_policy | day, night, schedule | night | 4/4 | The mode which the profile is applied to. |
| i<0~(m-1)>_begintime | hh:mm | 18:00 | 4/4 | Begin time of schedule mode. |
| i<0~(m-1)>_endtime | hh:mm | 06:00 | 4/4 | End time of schedule mode. |
| i<0~(m-1)>_win_i<0~4>_enable | <boolean> | 0 | 4/4 | Enable motion window. |
| i<0~(m-1)>_win_i<0~4>_name | string[14] | <blank> | 4/4 | Name of motion window. |
| i<0~(m-1)>_win_i<0~4>_ polygon | 0 ~ 320,0 ~ 240, 0 ~ 320,0 ~ 240, 0 ~ 320,0 ~ 240, 0 ~ 320,0 ~ 240 | 0 | 4/4 | Coordinate of polygon window position. (4 points: x0,y0,x1,y1,x2,y2,x3,y3) |
| i<0~(m-1)>_win_i<0~4>_objsize | 0 ~ 100 | 0 | 4/4 | Percent of motion detection window. |
| i<0~(m-1)>_win_i<0~4>_sensitivity | 0 ~ 100 | 0 | 4/4 | Sensitivity of motion detection window. |

# 7.17 Tempering detection settings

Group: **tampering_c<0~(n-1)>** for n channel product (capability.tampering > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 4/4 | Enable or disable tamper detection. |
| threshold | 0 ~ 255 | 32 | 1/6 | Threshold of tamper detection. |
| duration | 10 ~ 600 | 10 | 4/4 | If tampering value exceeds the 'threshold' for more than 'duration' second(s), then tamper detection is triggered. |

# 7.18 DDNS

Group: **ddns**

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 6/6 | Enable or disable the dynamic DNS. |
| provider | Safe100, DyndnsDynamic, DyndnsCustom, DynInterfree, CustomSafe100, | DyndnsDynamic | 6/6 | Safe100 => safe100.net<br>DyndnsDynamic => dyndns.org (dynamic)<br>DyndnsCustom => dyndns.org (custom)<br>DynInterfree =>dyn-interfree.it<br>CustomSafe100 =><br>Custom server using safe100 method |
| <provider>_hostname | string[128] | <blank> | 6/6 | Your DDNS hostname. |
| <provider>_usernameemail | string[64] | <blank> | 6/6 | Your user name or email to login to the DDNS service provider |
| <provider>_passwordkey | string[64] | <blank> | 6/6 | Your password or key to login to the DDNS service provider. |
| <provider>_servername | string[128] | <blank> | 6/6 | The server name for safe100.<br>(This field only exists if the provider is customsafe100) |

# 7.19 Express link

Group: expresslink

| PARAMETER | VALUE | Default | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 6/6 | Enable or disable express link. |
| state | onlycheck, onlyoffline, checkonline, badnetwork | NULL | 6/6 | Camera will check the status of network environment and express link URL |
| url | string[64] | NULL | 6/6 | The url user define to link to camera |

# 7.20 UPnP presentation

Group: upnppresentation

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 1 | 6/6 | Enable or disable the UPnP presentation service. |

# 7.21 UPnP port forwarding

Group: upnpportforwarding

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 6/6 | Enable or disable the UPnP port forwarding service. |
| upnpnatstatus | 0~3 | 0 | 6/7 | The status of UPnP port forwarding, used internally.<br>0 = OK, 1 = FAIL, 2 = no IGD router, 3 = no need for port forwarding |

# 7.22 System log

Group: **syslog**

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enableremotelog | <boolean> | 0 | 6/6 | Enable remote log. |
| serverip | <IP address> | <blank> | 6/6 | Log server IP address. |
| serverport | 514, 1025~65535 | 514 | 6/6 | Server port used for log. |
| level | 0~7 | 6 | 6/6 | Levels used to distinguish the importance of the information:<br>0: LOG_EMERG<br>1: LOG_ALERT<br>2: LOG_CRIT<br>3: LOG_ERR<br>4: LOG_WARNING<br>5: LOG_NOTICE<br>6: LOG_INFO |

| | | | | |
|---|---|---|---|---|
| | | | | 7: LOG_DEBUG |
| setparamlevel | 0~2 | 0 | 6/6 | Show log of parameter setting.<br>0: disable<br>1: Show log of parameter setting set from external.<br>2. Show log of parameter setting set from external and internal. |

# 7.23 SNMP

Group: **snmp** (capability.snmp > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| v2 | 0~1 | 0 | 6/6 | SNMP v2 enabled. 0 for disable, 1 for enable |
| v3 | 0~1 | 0 | 6/6 | SNMP v3 enabled. 0 for disable, 1 for enable |
| secnamerw | string[31] | Private | 6/6 | Read/write security name |
| secnamero | string[31] | Public | 6/6 | Read only security name |
| authpwrw | string[8~128] | <blank> | 6/6 | Read/write authentication password |
| authpwro | string[8~128] | <blank> | 6/6 | Read only authentication password |
| authtyperw | MD5,SHA | MD5 | 6/6 | Read/write authentication type |
| authtypero | MD5,SHA | MD5 | 6/6 | Read only authentication type |
| encryptpwrw | string[8~128] | <blank> | 6/6 | Read/write passwrd |
| encryptpwro | string[8~128] | <blank> | 6/6 | Read only password |
| encrypttyperw | DES | DES | 6/6 | Read/write encryption type |
| encrypttypero | DES | DES | 6/6 | Read only encryption type |
| rwcommunity | string[31] | Private | 6/6 | Read/write community |
| rocommunity | string[31] | Public | 6/6 | Read only community |
| syslocation | 0~128 | <blank> | 6/6 | System location |
| syscontact | 0~128 | <blank> | 6/6 | System contact |

# 7.24 Layout configuration

Group: **layout** (New version)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| logo_default | <boolean> | 1 | 1/6 | 0 => Custom logo<br>1 => Default logo |
| logo_link | string[64] | http://www.vivotek.com | 1/6 | Hyperlink of the logo |
| logo_powerbyvvtk_hidden | <boolean> | 0 | 1/6 | 0 => display the power by vivotek logo<br>1 => hide the power by vivotek logo |
| custombutton_manualtrigger_show<br><product dependent> | <boolean> | 1 | 1/6 | Show or hide manual trigger (VI) button in homepage<br>0 -> Hidden<br>1 -> Visible |
| theme_option | 1~4 | 1 | 1/6 | 1~3: One of the default themes.<br>4: Custom definition. |
| theme_color_font | string[7] | #ffffff | 1/6 | Font color |
| theme_color_configfont | string[7] | #ffffff | 1/6 | Font color of configuration area. |
| theme_color_titlefont | string[7] | #098bd6 | 1/6 | Font color of video title. |
| theme_color_controlbackground | string[7] | #565656 | 1/6 | Background color of control area. |
| theme_color_configbackground | string[7] | #323232 | 1/6 | Background color of configuration area. |
| theme_color_videobackground | string[7] | #565656 | 1/6 | Background color of video area. |
| theme_color_case | string[7] | #323232 | 1/6 | Frame color |

# 7.25 Privacy mask

Group: **privacymask_c<0~(n-1)>** for n channel product

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 4/4 | Enable privacy mask. |
| win_i<0~4>_enable | <boolean> | 0 | 4/4 | Enable privacy mask window. |
| win_i<0~4>_name | string[14] | <blank> | 4/4 | Name of the privacy mask window. |
| win_i<0~4>_ polygon | 0 ~ 320,0 ~ 240, 0 ~ 320,0 ~ 240, 0 ~ 320,0 ~ 240, 0 ~ 320,0 ~ 240 | 0 | 4/4 | Coordinate of polygon window position. (4 points: x0,y0,x1,y1,x2,y2,x3,y3) |

# 7.26 Capability

Group: capability

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| api_httpversion | <string> | 0100a | 0/7 | The HTTP API version. |
| bootuptime | <positive integer> | 60 | 0/7 | Server bootup time. |
| nir | 0, <positive integer> | 0 | 0/7 | Number of IR interfaces. (Recommand to use ir for built-in IR and extir for external IR) |
| npir | 0, <positive integer> | 0 | 0/7 | Number of PIRs. |
| ndi | 0, <positive integer> | 1 | 0/7 | Number of digital inputs. |
| nvi | 0, <positive integer> | 3 | 0/7 | Number of virtual inputs (manual trigger) |
| ndo | 0, <positive integer> | 1 | 0/7 | Number of digital outputs. |

| | | | | |
|---|---|---|---|---|
| naudioin | 0, <positive integer> | 1 | 0/7 | Number of audio inputs. |
| naudioout | 0, <positive integer> | 1 | 0/7 | Number of audio outputs. |
| nvideoin | <positive integer> | 1 | 0/7 | Number of video inputs. |
| nmediastream | <positive integer> | 3 | 0/7 | Number of media stream per channels. |
| nvideosetting | <positive integer> | 3 | 0/7 | Number of video settings per channel. |
| naudiosetting | <positive integer> | 1 | 0/7 | Number of audio settings per channel. |
| nuart | 0, <positive integer> | 0 | 0/7 | Number of UART interfaces. |
| nvideoinprofile | <positive integer> | 1 | 0/7 | Number of video input profiles. |
| nmotion | 0, <positive integer> | 5 | 0/7 | Number of motion window. |
| nmotionprofile | 0, <positive integer> | 1 | 0/7 | Number of motion profiles. |
| ptzenabled | 0, <positive integer> | 0 | 0/7 | An 32-bit integer, each bit can be set separately as follows:<br>Bit 0 => Support camera control function; 0(not support), 1(support)<br>Bit 1 => Built-in or external camera; 0(external), 1(built-in)<br>Bit 2 => Support pan operation, 0(not support), 1(support)<br>Bit 3 => Support tilt operation; 0(not support), 1(support)<br>Bit 4 => Support zoom operation; 0(not support), 1(support)<br>Bit 5 => Support focus operation; 0(not support), 1(support)<br>Bit 6 => Support iris operation; 0(not support), 1(support)<br>Bit 7 => External or built-in PT; 0(built-in), |

| | | | | |
|---|---|---|---|---|
| | | | | 1(external)<br>Bit 8 => Invalidate bit 1 ~ 7;<br>0(bit 1 ~ 7 are valid),<br>1(bit 1 ~ 7 are invalid)<br>Bit 9 => Reserved bit; Invalidate lens_pan, Lens_tilt, lens_zoon, lens_focus, len_iris.<br>0(fields are valid),<br>1(fields are invalid) |
| evctrlchannel | <boolean> | 1 | 0/7 | Indicate whether to support HTTP tunnel for event/control transfer. |
| joystick | <boolean> | 0 | 0/7 | Indicate whether to support joystick control. |
| storage_dbenabled | <boolean> | 1 | 0/7 | Media files are indexed in database. |
| ptzenabledclient | <boolean> | 0 | 0/7 | Indicate whether to support ptz client |
| protocol_https | < boolean > | 1 | 0/7 | Indicate whether to support HTTP over SSL. |
| protocol_rtsp | < boolean > | 1 | 0/7 | Indicate whether to support RTSP. |
| protocol_sip | <boolean> | 1 | 0/7 | Indicate whether to support SIP. |
| protocol_maxconnection | <positive integer> | 10 | 0/7 | The maximum allowed simultaneous connections. |
| protocol_maxgenconnection | <positive integer> | 10 | 0/7 | The maximum general streaming connections . |
| protocol_maxmegaconnection | <positive integer> | 0 | 0/7 | The maximum megapixel streaming connections. |
| protocol_rtp_multicast_ scalable | <boolean> | 1 | 0/7 | Indicate whether to support scalable multicast. |
| protocol_rtp_multicast_ backchannel | <boolean> | 0 | 0/7 | Indicate whether to support backchannel multicast. |
| protocol_rtp_tcp | <boolean> | 1 | 0/7 | Indicate whether to support RTP over TCP. |
| protocol_rtp_http | <boolean> | 1 | 0/7 | Indicate whether to support RTP over HTTP. |
| protocol_spush_mjpeg | <boolean> | 1 | 0/7 | Indicate whether to support server push MJPEG. |
| protocol_snmp | <boolean> | 1 | 0/7 | Indicate whether to support SNMP. |
| protocol_ipv6 | <boolean> | 1 | 0/7 | Indicate whether to support IPv6. |
| protocol_pppoe | <boolean> | 1 | 0/7 | Indicate whether to support PPPoE. |
| protocol_qos_cos | <boolean> | 1 | 0/7 | Indicate whether to support CoS. |
| protocol_qos_dscp | <boolean> | 1 | 0/7 | Indicate whether to support QoS/DSCP. |

| | | | | |
|---|---|---|---|---|
| videoin_type | 0, 1, 2 | 2 | 0/7 | 0 => Interlaced CCD<br>1 => Progressive CCD<br>2 => CMOS |
| videoin_resolution | <a list of available resolution separated by commas> <product dependent> | '192x192, 256x256, 384x384, 512x512, 768x768, 1056x1056 , 1280x1280 , 1536x1536 1920x1920 | 0/7 | Available resolutions list. |
| videoin_resolution16x9 | <a list of available resolution separated by commas> <product dependent> | 176x144, 384x216, 640x360, 1280x720, 1360x768, 1600x904, 1920x1080 | 0/7 | Available 16x9 resolutions list. |
| videoin_resolution1x1 | <a list of available resolution separated by commas> <product dependent> | '192x192, 256x256, 384x384, 512x512, 768x768, 1056x1056 , 1280x1280 , 1536x1536 1920x1920 | 0/7 | Available 1x1 resolutions list. |
| videoin_nresolution | < number of available resolution list> <product dependent> | 9 | 0/7 | Available resolutions list. (only for 5M series) |
| videoin_mpeg4_maxframerate | <a list of available | 15,15,15,15,15,15,15, | 0/7 | Available maximum frame list. (only for 5M series) |

| | | | | |
|---|---|---|---|---|
| | maximum frame rate separated by commas> <product dependent> | 15,15 | | |
| videoin_mjpeg_maxframerate | <a list of available maximum frame rate separated by commas> <product dependent> | 15,15,15,15,15,15,15,15,15,15 | 0/7 | Available maximum frame list. (only for 5M series) |
| videoin_h264_maxframerate | <a list of available maximum frame rate separated by commas> <product dependent> | 15,15,15,15,15,15,15,15,15,15 | 0/7 | Available maximum frame list. (only for 5M series) |
| videoin_svc_maxframerate | <a list of available maximum frame rate separated by commas> <product dependent> | 15,15,15,15,15,15,15,15,15,15 | 0/7 | Available maximum frame list. (only for 5M series) |
| videoin_streamcodec | < 1 ~ 15, 1~15, 1~15 (3 streams) > <product dependent> | 15,7,7 | 0/7 | Available stream codectype (Bit 0 -> mpeg4, Bit 1 -> mjpeg, Bit 2 -> h264, Bit 3 -> svc). (only for 5M series) |
| videoin_fov | <a list of available crop size separated by | 1920x1080,1952x1944 | 0/7 | Available crop size list. (only for 5M series) |

| | | | | |
|---|---|---|---|---|
| | commas><br><product dependent> | | | |
| videoin_maxframerate | <a list of available maximum frame rate separated by commas><br><product dependent> | 15,<br>15,<br>15,<br>15,<br>15,<br>15,<br>15,<br>15 | 0/7 | Available maximum frame list. |
| videoin_codec | mpeg4.<br>mjpeg, h264, svc<br><product dependent> | mpeg4,<br>mjpeg,<br>h264,<br>svc | 0/7 | Available codec list. |
| videoout_codec | <a list of the available codec types separated by commas)<br><product dependent> | <blank> | 0/7 | Available codec list. |
| timeshift | <boolean> | 1 | 0/7 | Indicate whether to support time shift caching stream. |
| audio_aec | <boolean> | 0 | 0/7 | Indicate whether to support acoustic echo cancellation. |
| audio_extmic | <boolean> | 1 | 0/7 | Indicate whether to support external microphone input. |
| audio_linein | <boolean> | 1 | 0/7 | Indicate whether to support external line input.<br>(It will be replaced by audio_mic and audio_extmic.) |
| audio_lineout | <boolean> | 1 | 0/7 | Indicate whether to support line output. |
| audio_headphoneout | <boolean> | 0 | 0/7 | Indicate whether to support headphone output. |
| audioin_codec | aac4, gamr, g711<br><product | aac4, gamr, g711 | 0/7 | Available codec list for audio input. |

| | | | | |
|---|---|---|---|---|
| | dependent> | | | |
| audioout_codec | g711 <product dependent> | <blank> | 0/7 | Available codec list for SIP. |
| camctrl_httptunnel | <boolean> | 0 | 0/7 | Indicate whether to support httptunnel. |
| camctrl_httptunnelclient | <boolean> | 0 | 0/7 | Indicate whether to support httptunnel client. |
| camctrl_privilege | <boolean> | 1 | 0/7 | Indicate whether to support "Manage Privilege" of PTZ control in the Security page.<br>1: support both /cgi-bin/camctrl/camctrl.cgi and /cgi-bin/viewer/camctrl.cgi<br>0: support only /cgi-bin/viewer/camctrl.cgi |
| uart_httptunnel | <boolean> | 0 | 0/7 | Indicate whether to support HTTP tunnel for UART transfer. |
| transmission_mode | Tx,<br>Rx,<br>Both | Tx | 0/7 | Indicate transmission mode of the machine: TX = server, Rx = receiver box, Both = DVR. |
| network_wire | <boolean> | 1 | 0/7 | Indicate whether to support Ethernet. |
| network_wireless | <boolean> | 0 | 0/7 | Indicate whether to support wireless. |
| wireless_s802dot11b | <boolean> | 0 | 0/7 | Indicate whether to support wireless 802.11b+. |
| wireless_s802dot11g | <boolean> | 0 | 0/7 | Indicate whether to support wireless 802.11g. |
| wireless_encrypt_wep | <boolean> | 0 | 0/7 | Indicate whether to support wireless WEP. |
| wireless_encrypt_wpa | <boolean> | 0 | 0/7 | Indicate whether to support wireless WPA. |
| wireless_encrypt_wpa2 | <boolean> | 0 | 0/7 | Indicate whether to support wireless WPA2. |
| wireless_beginchannel | 1 ~ 14 | 255 | 0/7 | Indicate the begin channel of wireless network |
| wireless_endchannel | 1 ~ 14 | 255 | 0/7 | Indicate the end channel of wireless network |

| | | | | |
|---|---|---|---|---|
| derivative_brand | <boolean> | 1 | 0/7 | Indicate whether to support the upgrade function for the derivative brand. For example, if the value is true, the VVTK product can be upgraded to VVXX. (TCVV<->TCXX is excepted) |
| npreset | 0, <positive integer> | 20 | 0/7 | Number of preset locations |
| eptz | 0, <positive integer> | 7 | 0/7 | A 32-bit integer, each bit can be set separately as follows:<br>Bit 0 => stream 1 supports ePTZ or not.<br>Bit 1 => stream 2 supports ePTZ or not.<br>The rest may be deduced by analogy |
| nanystream | 0, <positive integer> | 0 | 0/7 | number of any media stream per channel |
| iva | <boolean> | 0 | 0/7 | Indicate whether to support Intelligent Video analysis |
| tampering | <boolean> | 1 | 0/7 | Indicate whether to support tampering detection. |
| test_ac | <boolean> | 1 | 0/7 | Indicate whether to support test ac key. |
| version_onvifdaemon | <string> | 1.7.1.1 | 0/7 | Indicate ONVIF daemon version |
| image_wdrc | <Boolean> | 1 | 0/7 | Indicate whether to support WDR enhanced. |
| image_ iristype | <string> | <blank> | 0/7 | Indicate iris type. |
| image_ focusassist | <Boolean> | 0 | 0/7 | Indicate whether to support focus assist. |
| fisheye | <Boolean> | 1 | 0/7 | Indicate fisheye model. |
| localstorage_manageable | <boolean> | 1 | 0/7 | Indicate whether manageable local storage is supported. |
| localstorage_seamless | <boolean> | 1 | 0/7 | Indicate whether seamless recording is supported. |
| localstorage_modnum | 0, <positive integer> | 4 | 0/7 | The maximum MOD connection numbers. |

| | | | | |
|---|---|---|---|---|
| localstorage_slconnum | 0, <positive integer> | 1 | 0/7 | The maximum seamless connection number. |
| adaptiverecording | <boolean> | 1 | 0/7 | Indicate whether to support adaptive recording. |
| adaptivestreaming | <boolean> | 1 | 0/7 | Indicate whether to support adaptive streaming. |
| supportsd | <boolean> | 1 | 0/7 | Indicate whether to support local storage. |
| remotecamctrl_master | 0, <positive integer> | 1 | 0/7 | Indicate whether to support remote auxiliary camera (master side), this value means supporting max number of auxiliary camera. |
| remotecamctrl_slave | <booleam> | 0 | 0/7 | Indicate whether to support remote camera control (slave side). |

# 7.27 Customized event script

Group: event_customtaskfile_i<0~2>

| PARAMETER | VALUE | Default | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| name | string[41] | <blank> | 6/7 | Custom script identification of this entry. |
| date | string[17] | <blank> | 6/7 | Date of custom script. |
| time | string[17] | <blank> | 6/7 | Time of custom script. |

# 7. 280 Event setting

Group: **event_i**<0~2>

| PARAMETER | VALUE | Default | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| name | string[40] | <blank> | 6/6 | Identification of this entry. |
| enable | 0, 1 | 0 | 6/6 | Enable or disable this event. |
| priority | 0, 1, 2 | 1 | 6/6 | Indicate the priority of this event:<br>"0" = low priority<br>"1" = normal priority<br>"2" = high priority |

| | | | | |
|---|---|---|---|---|
| delay | 1~999 | 20 | 6/6 | Delay in seconds before detecting the next event. |
| trigger | boot,<br>di,<br>motion,<br>seq,<br>recnotify,<br>tampering,<br>visignal,<br>vi | boot | 6/6 | Indicate the trigger condition:<br>"boot" = System boot<br>"di"= Digital input<br>"motion" = Video motion detection<br>"seq" = Periodic condition<br>"visignal" = Video input signal loss.<br>"recnotify" = Recording notification.<br>"tampering" = Tamper detection.<br>"vi"= Virtual input (Manual trigger) |
| triggerstatus | String[40] | trigger | 6/6 | The status for event trigger |
| di | <integer> | 1 | 6/6 | Indicate the source id of di trigger.<br>This field is required when trigger condition is "di".<br>One bit represents one digital input.<br>The LSB indicates DI 0. |
| mdwin | <integer> | 0 | 6/6 | Indicate the source window id of motion detection.<br>This field is required when trigger condition is "md".<br>One bit represents one window.<br>The LSB indicates the 1st window.<br>For example, to detect the 1st and 3rd windows, set mdwin as 5. |
| mdwin0 | <integer> | 0 | 6/6 | Similar to mdwin. The parameter takes effect when profile 1 of motion detection is enabled. |
| vi | <integer> | 0 | 6/6 | Indicate the source id of vi trigger.<br>This field is required when trigger condition is "vi".<br>One bit represents one digital input.<br>The LSB indicates VI 0. |
| inter | 1~999 | 1 | 6/6 | Interval of snapshots in minutes.<br>This field is used when trigger condition is "seq". |

| | | | | |
|---|---|---|---|---|
| weekday | 0~127 | 127 | 6/6 | Indicate which weekday is scheduled.<br>One bit represents one weekday.<br>bit0 (LSB) = Saturday<br>bit1 = Friday<br>bit2 = Thursday<br>bit3 = Wednesday<br>bit4 = Tuesday<br>bit5 = Monday<br>bit6 = Sunday<br>For example, to detect events on Friday and Sunday, set weekday as 66. |
| begintime | hh:mm | 00:00 | 6/6 | Begin time of the weekly schedule. |
| endtime | hh:mm | 24:00 | 6/6 | End time of the weekly schedule.<br>(00:00 ~ 24:00 sets schedule as always on) |
| lowlightcondition<br><product dependent> | 0, 1 | 1 | 6/6 | Switch on white light LED in low light condition<br>0 => Do action at all times<br>1 => Do action in low-light conditions |
| action_do_i<0~(ndo-1)>_enable | 0, 1 | 0 | 6/6 | Enable or disable trigger digital output. |
| action_do_i<0~(ndo-1)>_duration | 1~999 | 1 | 6/6 | Duration of the digital output trigger in seconds. |
| action_goto_enable<br><product dependent> | <Boolean> | 0 | 6/6 | Enable/disable ptz goto preset position on event triggered. |
| action_goto_name<br><product dependent> | string[40] | <blank> | 6/6 | Specify the preset name that ptz goto on event triggered. |
| action_cf_enable | <Boolean> | 0 | 6/6 | Enable or disable sending media to SD card. |
| action_cf_folder | string[128] | <blank> | 6/6 | Path to store media. |
| action_cf_media | NULL, 0~4 | <blank> | 6/6 | Index of the attached media. |
| action_cf_datefolder | <boolean> | 0 | 6/6 | Enable this to create folders by date, time, and hour automatically. |
| action_cf_backup | <Boolean> | 0 | 6/6 | Enable or disable the function that send media to SD card for backup if network is disconnected. |
| action_server_i<0~4>_enable | 0, 1 | 0 | 6/6 | Enable or disable this server action. |

| | | | | |
|---|---|---|---|---|
| action_server_i<0~4>_ media | NULL, 0~4 | <blank> | 6/6 | Index of the attached media. |
| action_server_i<0~4>_ datefolder | <boolean> | 0 | 6/6 | Enable this to create folders by date, time, and hour automatically. |
| action_patrol_enable (only for VS series) <product dependent> | <Boolean> | 0 | 6/6 | Enable/disable ptz patrol when event triggered. |
| action_ patrol _server (only for VS series) <product dependent> | 0~255 | 0 | 6/6 | Indicate the target servers to which the snapshots taken during patrol dwelling time should be sent.<br>One bit represents one application server (server_i0~i4).<br>bit0 (LSB) = server_i0.<br>bit1 = server_i1.<br>bit2 = server_i2.<br>bit3 = server_i3.<br>bit4 = server_i4.<br>For example, enable server_i0, server_i2, and server_i4 as notification servers; the notifyserver value is 21. |

# 7.29 Server setting for event action

Group: **server_i**<0~4>

| PARAMETER | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| name | string[40] | NULL | 6/6 | Identification of this entry |
| type | email,<br>ftp,<br>http,<br>ns | email | 6/6 | Indicate the server type:<br>“email” = email server<br>“ftp” = FTP server<br>“http” = HTTP server<br>“ns” = network storage |
| http_url | string[128] | http:// | 6/6 | URL of the HTTP server to upload. |
| http_username | string[64] | NULL | 6/6 | Username to log in to the server. |
| http_passwd | string[64] | NULL | 6/6 | Password of the user. |
| ftp_address | string[128] | NULL | 6/6 | FTP server address. |
| ftp_username | string[64] | NULL | 6/6 | Username to log in to the server. |

| | | | | |
|---|---|---|---|---|
| ftp_passwd | string[64] | NULL | 6/6 | Password of the user. |
| ftp_port | 0~65535 | 21 | 6/6 | Port to connect to the server. |
| ftp_location | string[128] | NULL | 6/6 | Location to upload or store the media. |
| ftp_passive | 0, 1 | 1 | 6/6 | Enable or disable passive mode.<br>0 = disable passive mode<br>1 = enable passive mode |
| email_address | string[128] | NULL | 6/6 | Email server address. |
| email_sslmode | 0, 1 | 0 | 6/6 | Enable support SSL. |
| email_port | 0~65535 | 25 | 6/6 | Port to connect to the server. |
| email_username | string[64] | NULL | 6/6 | Username to log in to the server. |
| email_passwd | string[64] | NULL | 6/6 | Password of the user. |
| email_senderemail | string[128] | NULL | 6/6 | Email address of the sender. |
| email_recipientemail | string[128] | NULL | 6/6 | Email address of the recipient. |
| ns_location | string[128] | NULL | 6/6 | Location to upload or store the media. |
| ns_username | string[64] | NULL | 6/6 | Username to log in to the server. |
| ns_passwd | string[64] | NULL | 6/6 | Password of the user. |
| ns_workgroup | string[64] | NULL | 6/6 | Workgroup for network storage. |

# 7.30 Media setting for event action

Group: **media_i<0~4>** (media_freespace is used internally.)

| PARAMETER | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| name | string[40] | NULL | 6/6 | Identification of this entry |
| type | snapshot,<br>systemlog,<br>videoclip,<br>recordmsg | snapshot | 6/6 | Media type to send to the server or store on the server. |
| snapshot_source | <integer> | 0 | 6/6 | Indicate the source of media stream.<br>0 means the first stream.<br>1 means the second stream and etc.<br>2 means the third stream and etc.<br>3 means the fourth stream and etc. |

| | | | | |
|---|---|---|---|---|
| snapshot_prefix | string[16] | Snapshot1_ | 6/6 | Indicate the prefix of the filename.<br>media_i0=> Snapshot1_<br>media_i1=> Snapshot2_<br>media_i2=> Snapshot3_<br>media_i3=> Snapshot4_<br>media_i4=> Snapshot5_ |
| snapshot_datesuffix | 0, 1 | 0 | 6/6 | Add date and time suffix to filename:<br>1 = Add date and time suffix.<br>0 = Do not add. |
| snapshot_preevent | 0 ~ 7 | 1 | 6/6 | Indicates the number of pre-event images. |
| snapshot_postevent | 0 ~ 7 | 1 | 6/6 | The number of post-event images. |
| videoclip_source | <integer> | 0 | 6/6 | Indicate the source of media stream.<br>0 means the first stream.<br>1 means the second stream and etc.<br>2 means the third stream and etc.<br>3 means the fourth stream and etc. |
| videoclip_prefix | string[16] | VideoClip1_ | 6/6 | Indicate the prefix of the filename. |
| videoclip_preevent | 0 ~ 9 | 0 | 6/6 | Indicates the time for pre-event recording in seconds. |
| videoclip_maxduration | 1 ~ 20 | 5 | 6/6 | Maximum duration of one video clip in seconds. |
| videoclip_maxsize | 50 ~ 8192 | 1000 | 6/6 | Maximum size of one video clip file in Kbytes. |

# 7.31 Recording

Group: **recording_i**<0~1>

| PARAMETER | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| name | string[40] | NULL | 6/6 | Identification of this entry. |
| trigger | schedule, networkfail | schedule | 6/6 | The event trigger type<br>schedule: The event is triggered by schedule<br>networkfail: The event is triggered by the failure of network connection. |
| enable | 0, 1 | 0 | 6/6 | Enable or disable this recording. |

| | | | | |
|---|---|---|---|---|
| priority | 0, 1, 2 | 1 | 6/6 | Indicate the priority of this recording:<br>"0" indicates low priority.<br>"1" indicates normal priority.<br>"2" indicates high priority. |
| source | 0~3 | 0 | 6/6 | Indicate the source of media stream.<br>0 means the first stream.<br>1 means the second stream and so on. |
| limitsize | 0,1 | 0 | 6/6 | 0: Entire free space mechanism<br>1: Limit recording size mechanism |
| cyclic | 0,1 | 0 | 6/6 | 0: Disable cyclic recording<br>1: Enable cyclic recording |
| notify | 0,1 | 1 | 6/6 | 0: Disable recording notification<br>1: Enable recording notification |
| notifyserver | 0~31 | 0 | 6/6 | Indicate which notification server is scheduled.<br>One bit represents one application server (server_i0~i4).<br>bit0 (LSB) = server_i0.<br>bit1 = server_i1.<br>bit2 = server_i2.<br>bit3 = server_i3.<br>bit4 = server_i4.<br>For example, enable server_i0, server_i2, and server_i4 as notification servers; the notifyserver value is 21. |
| weekday | 0~127 | 127 | 6/6 | Indicate which weekday is scheduled.<br>One bit represents one weekday.<br>bit0 (LSB) = Saturday<br>bit1 = Friday<br>bit2 = Thursday<br>bit3 = Wednesday<br>bit4 = Tuesday<br>bit5 = Monday<br>bit6 = Sunday<br>For example, to detect events on Friday and Sunday, set weekday as 66. |
| begintime | hh:mm | 00:00 | 6/6 | Start time of the weekly schedule. |

| | | | | |
|---|---|---|---|---|
| endtime | hh:mm | 24:00 | 6/6 | End time of the weekly schedule. (00:00~24:00 indicates schedule always on) |
| prefix | string[16] | <blank> | 6/6 | Indicate the prefix of the filename. |
| cyclesize | 200~ | 100 | 6/6 | The maximum size for cycle recording in Kbytes when choosing to limit recording size. (not used in FE8171) |
| reserveamount | 0~ | 100 | 6/6 | The reserved amount in Mbytes when choosing cyclic recording mechanism. |
| dest | cf,<br>0~4 | cf | 6/6 | The destination to store the recorded data.<br>"cf" means local storage (CF or SD card).<br>"0" means the index of the network storage. |
| cffolder | string[128] | NULL | 6/6 | Folder name. |
| filesize | 100~900 | 100 | 6/6 | Unit: Mega bytes.<br>When this condition is reached, recording file is truncated. |
| duration | 1~30 | 1 | 6/6 | Uuit: Minute<br>When this condition is reached, recording file is truncated. |
| adaptive_enable <product dependent> | 0,1 | 0 | 6/6 | Indicate whether the adaptive recording is enabled |
| adaptive_preevent <product dependent> | 0~9 | 1 | 6/6 | Indicate when is the adaptive recording started before the event trigger point (seconds) |
| adaptive_postevent <product dependent> | 0~10 | 1 | 6/6 | Indicate when is the adaptive recording stopped after the event trigger point (seconds) |

# 7.32 HTTPS

Group: **https** (capability.protocol.https > 0)

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 6/6 | To enable or disable secure HTTP. |
| policy | <Boolean> | 0 | 6/6 | If the value is 1, it will force HTTP connection redirect to HTTPS connection |
| method | auto,<br>manual,<br>install | auto | 6/6 | auto => Create self-signed certificate automatically.<br>manual => Create self-signed certificate manually.<br>install => Create certificate request and install. |
| status | -3 ~ 1 | 0 | 6/7 | Specify the https status.<br>-3 = Certificate not installed<br>-2 = Invalid public key<br>-1 = Waiting for certificate<br>0 = Not installed<br>1 = Active |
| countryname | string[2] | TW | 6/6 | Country name in the certificate information. |
| stateorprovincename | string[128] | Asia | 6/6 | State or province name in the certificate information. |
| localityname | string[128] | Asia | 6/6 | The locality name in the certificate information. |
| organizationname | string[64] | Vivotek.Inc | 6/6 | Organization name in the certificate information. |
| unit | string[32] | Vivotek.Inc | 6/6 | Organizational unit name in the certificate information. |
| commonname | string[64] | www.vivotek.com | 6/6 | Common name in the certificate information. |
| validdays | 0 ~ 3650 | 3650 | 6/6 | Valid period for the certification. |

# 7.33 Storage management setting

Currently it's for local storage (SD, CF card)

Group: **disk_i<0~(n-1)>** n is the total number of storage devices. (capability.storage.dbenabled > 0)

| PARAMETER | VALUE | Default | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| cyclic_enabled | <boolean> | 0 | 6/6 | Enable cyclic storage method. |
| autocleanup_enabled | <boolean> | 0 | 6/6 | Enable automatic clean up method. Expired and not locked media files will be deleted. |
| autocleanup_maxage | <positive integer> | 7 | 6/6 | To specify the expired days for automatic clean up. |

# 7.34 ePTZ setting

Group: **eptz_c<0~(n-1)>** for n channel product. (capability.eptz > 0)

| PARAMETER | VALUE | Default | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| tiltspeed | -5 ~ 5 | 0 | 1/4 | Tilt speed |
| panspeed | -5 ~ 5 | 0 | 1/4 | Pan speed |
| zoomspeed | -5 ~ 5 | 0 | 1/4 | Zoom speed |
| panoramicspeed | 1 ~ 5 | 1 | 1/4 | Panoramic speed |
| rotatespeed | 1 ~ 5 | 1 | 1/4 | Rotate speed |

Group: **eptz_c<0~(n-1)>_s<0~(m-1)>** for n channel product and m is the number of streams which support ePTZ. (capability.eptz > 0)

| PARAMETER | VALUE | Default | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| patrolseq | string[120] | <blank> | 1/4 | The patrol sequence of ePTZ. All the patrol position indexes will be separated by "," |
| preset_i<0~19>_name | string[40] | <blank> | 1/4 | Name of ePTZ preset. |
| preset_i<0~19>_pos | <coordinate> | <blank> | 1/4 | Coordinate of the preset. (It should be get from plugin: x, y, z, zfactor, scroll) |

# 7.35 Fisheye info

Group: **fisheyeinfo**

| NAME | VALUE | DEFAULT | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| revisedcenteraxis | <coordinate> | <product dependent> | 6/99 | The actual center axis coordinate |
| radius | <integer> | <product dependent> | 6/99 | The actual center radius |

# 7.36 Seamless recording setting

Group: **seamlessrecording** (capability.localstorage.seamless > 0)

| PARAMETER | VALUE | Default | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| diskmode | seamless, manageable | seamless | 1/6 | "seamless" indicates enable seamless recording.<br>"manageable" indicates disable seamless recording. |
| maxconnection | 3 | 3 | 1/6 | Maximum number of connected seamless streaming. |
| stream | 1~3 | 3 | 1/6 | (Internal used, read only) |
| output | 0~3 | 2 | 1/6 | (Internal used, read only) |
| enable | <boolean> | 0 | 1/6 | Indicate whether seamless recording is recording to local storage or not at present.<br>(Read only) |
| guid<0~2>_id | string[127] | <blank> | 1/6 | The connected seamless streaming ID.<br>(Read only) |
| guid<0~2>_number | 0~3 | 0 | 1/6 | Number of connected seamless streaming with guid<0~2>_id.<br>(Read only) |

# 7.37 Panoramic PTZ settings

Group:**ivas_c0** (capability_remotecamctrl_master > 0)

| PARAMETER | VALUE | Default | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 1 | 6/6 | Enable intelligence video analysis |

Group:**ivas_c0_objtrack** (capability_remotecamctrl_master > 0)

| PARAMETER | VALUE | Default | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 6/6 | Enable object tracking analytics |
| objsize | 0~10000,0~10000 | 312,312 | 6/6 | Minimal detected object size. Value="width,height". The value is the proportion of object in image size and expands to 10000. |
| sensitivity | 0~10000 | 6000 | 6/6 | Sensitivity of object detection window. |
| win_i0_enable | <boolean> | 0 | 6/6 | Enable this detection window |
| win_i0_name | String[40] | <blank> | 6/6 | Name of detection window |
| win_i0_polygon | 0~10000 | 0,0, 10000,0, 10000,10000, 0,10000 | 6/6 | Coordinate of polygon window position. Valid coordinate number of polygon points: 3~20. Example: (points:x0,y0,x1,y1,x2,y2,x3,y3, …) |

Group:**remotecamctrl_c0** (capability_remotecamctrl_master > 0)

| PARAMETER | VALUE | Default | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 6/6 | Enable Panoramic PTZ |

Group:**remotecamctrl_c0_client**<0~(n-1)> (capability_remotecamctrl_master > 0)

| PARAMETER | VALUE | Default | SECURITY (get/set) | DESCRIPTION |
|---|---|---|---|---|
| enable | <boolean> | 0 | 6/6 | Enable Controller camera to control the Auxiliary one. |
| createtime | string[64] | <blank> | 6/99 | The creative time of uploaded map file. |

| | | | | |
|---|---|---|---|---|
| ip | <ip address> | <blank> | 6/6 | Ip address of Auxiliary camera. |
| port | 80,1025~65535 | <blank> | 6/6 | Connection port of Auxiliary camera. |
| account | string[64] | <blank> | 6/6 | User name of Auxiliary camera account. |
| passwd | string[128] | <blank> | 6/6 | Password of Auxiliary camera account. |
| eventalarm | 0~7 | 0 | 6/6 | Indicate the source id of auxiliary camera's manual trigger. The field is required when trigger condition is "manual" on auxiliary camera.<br>One bit represents one digital input. The LSB indicates VI 0. |
| nrmlinterval | 0~300 | 10 | 6/6 | When the last control finish after <nrmlinterval> seconds, controller camera will send manual trigger with normal signal to auxiliary camera. |

# 8. Useful Functions

## 8.1 Drive the Digital Output (capability.ndo > 0)

**Note:** This request requires Viewer privileges.

**Method:** GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/setdo.cgi?do1=<state>[&do2=<state>]
[&do3=<state>][&do4=<state>]
```

Where state is 0 or 1; "0" means inactive or normal state, while "1" means active or triggered state.

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| do<num> | 0, 1 | 0 – Inactive, normal state |
| | | 1 – Active, triggered state |

**Example:** Drive the digital output 1 to triggered state and redirect to an empty page.

http://myserver/cgi-bin/dido/setdo.cgi?do1=1

## 8.2 Query Status of the Digital Input (capability.ndi > 0)

Note: This request requires Viewer privileges

**Method:** GET/POST

Syntax:

```
http://<servername>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]
```

If no parameter is specified, all of the digital input statuses will be returned.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: <length>\r\n
\r\n
[di0=<state>]\r\n
[di1=<state>]\r\n
[di2=<state>]\r\n
[di3=<state>]\r\n
```

where <*state*> can be 0 or 1.

**Example:** Query the status of digital input 1 .

Request:

http://myserver/cgi-bin/dido/getdi.cgi?di1

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: 7\r\n

\r\n

di1=1\r\n

# 8.3 Query Status of the Digital Output (capability.ndo > 0)

**Note:** This request requires Viewer privileges

**Method:** GET/POST

Syntax:

http://<*servername*>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]

If no parameter is specified, all the digital output statuses will be returned.

Return:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: <*length*>\r\n

\r\n

[do0=<state>]\r\n

[do1=<state>]\r\n

[do2=<state>]\r\n

[do3=<state>]\r\n

where <*state*> can be 0 or 1.

**Example:** Query the status of digital output 1.

Request:

http://myserver/cgi-bin/dido/getdo.cgi?do1

Response:

HTTP/1.0 200 OK\r\n

Content-Type: text/plain\r\n

Content-Length: 7\r\n

```
\r\n
do1=1\r\n
```

# 8.4 Capture Single Snapshot

**Note:** This request requires Normal User privileges.

**Method:** GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>][&streamid=<value>]
```

If the user requests a size larger than all stream settings on the server, this request will fail.

| PARAMETER | VALUE | DEFAULT | DESCRIPTION |
|---|---|---|---|
| channel | 0~(n-1) | 0 | The channel number of the video source. |
| resolution | <available resolution> | 0 | The resolution of the image. |
| quality | 1~5 | 3 | The quality of the image. |
| streamid | 0~(m-1) | <product dependent> | The stream number. |

The server will return the most up-to-date snapshot of the selected channel and stream in JPEG format. The size and quality of the image will be set according to the video settings on the server.

Return:

```
HTTP/1.0 200 OK\r\n
Content-Type: image/jpeg\r\n
[Content-Length: <image size>\r\n]

<binary JPEG image data>
```

# 8.5 Account Management

**Note:** This request requires Administrator privileges.

**Method:** GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/editaccount.cgi?
method=<value>&username=<*name*>[&userpass=<*value*>][&privilege=<*value*>]
[&privilege=<value>][…][&return=<*return page*>]

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| method | Add | Add an account to the server. When using this method, the "username" field is necessary. It will use the default value of other fields if not specified. |
| | Delete | Remove an account from the server. When using this method, the "username" field is necessary, and others are ignored. |
| | edit | Modify the account password and privilege. When using this method, the "username" field is necessary, and other fields are optional. If not specified, it will keep the original settings. |
| username | <name> | The name of the user to add, delete, or edit. |
| userpass | <value> | The password of the new user to add or that of the old user to modify. The default value is an empty string. |
| Privilege | <value> | The privilege of the user to add or to modify. |
| | viewer | Viewer privilege. |
| | operator | Operator privilege. |
| | admin | Administrator privilege. |
| Return | <return page> | Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. |

# 8.6 System Logs

**Note:** This request require Administrator privileges.

**Method:** GET/POST

Syntax:

| |
|---|
| http://<*servername*>/cgi-bin/admin/syslog.cgi |

Server will return the most up-to-date system log.

Return:

| |
|---|
| HTTP/1.0 200 OK\r\n |
| Content-Type: text/plain\r\n |
| Content-Length: <syslog length>\r\n |
| \r\n |
| <system log information>\r\n |

# 8.7 Upgrade Firmware

**Note:** This request requires Administrator privileges.

Method: POST

Syntax:

| |
|---|
| http://<*servername*>/cgi-bin/admin/upgrade.cgi |

Post data:

| |
|---|
| fimage=<file name>[&return=<return page>]\r\n |
| \r\n |
| <multipart encoded form data> |

Server will accept the file named <file name> to upgrade the firmware and return with <return page> if indicated.

# 8.8 ePTZ Camera Control (capability.eptz > 0, not used in FE8171)

**Note:** This request requires camctrl privileges.

**Method:** GET/POST

Syntax:

http://<*servername*>/cgi-bin/camctrl/eCamCtrl.cgi?channel=<value>&stream=<value>
[&move=<value>] – Move home, up, down, left, right
[&auto=<value>] – Auto pan, patrol
[&zoom=<value>] – Zoom in, out
[&zooming=<value>&zs=<value>] – Zoom without stopping, used for joystick
[&vx=<value>&vy=<value>&vs=<value>] – Shift without stopping, used for joystick
[&x=<value>&y=<value>&videosize=<value>&resolution=<value>&stretch=<value>] – Click on image (Move the center of image to the coordination (x,y) based on resolution or videosize.)
[ [&speedpan=<value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>] ] – Set speeds
[&return=<return page>]

Example:

http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=0&move=right
http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&vx=2&vy=2&vz=2
http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&x=100&y=100&videosize=640x480&resolution=640x480&stretch=0

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| channel | <0~(n-1)> | Channel of video source. |
| stream | <0~(m-1)> | Stream. |
| move | home | Move to home ROI. |
| | up | Move up. |
| | down | Move down. |
| | left | Move left. |
| | right | Move right. |
| auto | pan | Auto pan. |
| | patrol | Auto patrol. |
| | stop | Stop auto pan/patrol. |

| | | |
|---|---|---|
| zoom | wide | Zoom larger view with current speed. |
| | tele | Zoom further with current speed. |
| zooming | wide or tele | Zoom without stopping for larger view or further view with zs speed, used for joystick control. |
| zs | 0 ~ 6 | Set the speed of zooming, "0" means stop. |
| vx | <integer> | The direction of movement, used for joystick control. |
| vy | <integer> | |
| vs | 0 ~ 7 | Set the speed of movement, "0" means stop. |
| x | <integer> | x-coordinate clicked by user.<br>It will be the x-coordinate of center after movement. |
| y | <integer> | y-coordinate clicked by user.<br>It will be the y-coordinate of center after movement. |
| videosize | <window size> | The size of plug-in (ActiveX) window in web page |
| resolution | <window size> | The resolution of streaming. |
| stretch | <boolean> | 0 indicates that it uses **resolution** (streaming size) as the range of the coordinate system.<br>1 indicates that it uses **videosize** (plug-in size) as the range of the coordinate system. |
| speedpan | -5 ~ 5 | Set the pan speed. |
| speedtilt | -5 ~ 5 | Set the tilt speed. |
| speedzoom | -5 ~ 5 | Set the zoom speed. |
| speedapp | 1 ~ 5 | Set the auto pan/patrol speed. |
| return | <return page> | Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. |

# 8.10 ePTZ Recall (capability.eptz > 0, not used in FE8171)

**Note:** This request requires camctrl privileges.

Method: GET/POST

Syntax:

| |
|---|
| http://<*servername*>/cgi-bin/camctrl/eRecall.cgi?channel=<value>&stream=<value>& recall=<value>[&return=<*return page*>] |

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| channel | <0~(n-1)> | Channel of the video source. |
| stream | <0~(m-1)> | Stream. |
| recall | Text string less than 40 characters | One of the present positions to recall. |
| return | <return page> | Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. |

# 8.11 ePTZ Preset Locations (capability.eptz > 0, not used in FE8171)

**Note:** This request requires Operator privileges.

**Method:** GET/POST

Syntax:

| |
|---|
| http://<*servername*>/cgi-bin/operator/ePreset.cgi?channel=<value>&stream=<value> [&addpos=<value>][&delpos=<value>][&return=<*return page*>] |

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| channel | <0~(n-1)> | Channel of the video source. |
| stream | <0~(m-1)> | Stream. |
| addpos | <Text string less than 40 characters> | Add one preset location to the preset list. |
| delpos | <Text string less than 40 characters> | Delete preset location from the preset list. |

| | | |
|---|---|---|
| return | <return page> | Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. |

# 8.12 IP Filtering

**Note:** This request requires Administrator access privileges.

**Method:** GET/POST

Syntax: <product dependent>

http://<*servername*>/cgi-bin/admin/ipfilter.cgi?type[=<value>]
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=add<v4/v6>&ip=<*ipaddress*>[&index=<value>][&return=<*return page*>]
http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=del<v4/v6>&index=<value>[&return=<*return page*>]

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| type | NULL | Get IP filter type |
| | allow, deny | Set IP filter type |
| method | addv4 | Add IPv4 address into access list. |
| | addv6 | Add IPv6 address into access list. |
| | delv4 | Delete IPv4 address from access list. |
| | delv6 | Delete IPv6 address from access list. |
| ip | <IP address> | Single address: <IP address><br>Network address: <IP address / network mask><br>Range address:<start IP address - end IP address> |
| index | <value> | The start position to add or to delete. |
| return | <return page> | Redirect to the page <*return page*> after the parameter is assigned. The <*return page*> can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. |

# 8.13 Event/Control HTTP Tunnel Channel (capability.evctrlchannel > 0)

**Note:** This request requires Administrator privileges.

**Method:** GET and POST

Syntax:

```
http://<servername>/cgi-bin/admin/ctrlevent.cgi
---------------------------------------------------------------------
GET /cgi-bin/admin/ctrlevent.cgi
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache


---------------------------------------------------------------------
POST /cgi-bin/admin/ ctrlevent.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT
```

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through the proxy server.

This channel will help perform real-time event subscription and notification as well as camera control more efficiently. The event and control formats are described in another document.

See Event/control tunnel spec for detail information

# 8.14 Get SDP of Streams

**Note:** This request requires Viewer access privileges.

**Method:** GET/POST

Syntax:

| |
|---|
| http://<*servername*>/<network_rtsp_s<0~m-1>_accessname> |

"m" is the stream number.

"network_accessname_<0~(m-1)>" is the accessname for stream "1" to stream "m". Please refer to the "subgroup of network: rtsp" for setting the accessname of SDP.

You can get the SDP by HTTP GET.

When using scalable multicast, Get SDP file which contains the multicast information via HTTP.

# 8.15 Open the Network Stream

**Note:** This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

| |
|---|
| http://<*servername*>/<network_http_s<0~m-1>_accessname> |

For RTSP (MP4), the user needs to input the URL below into an RTSP compatible player.

| |
|---|
| rtsp://<*servername*>/<network_rtsp_s<0~m-1>_accessname> |

"m" is the stream number.

For details on streaming protocol, please refer to the "control signaling" and "data format" documents.

# 8.16 Storage managements (capability.storage.dbenabled > 0)

**Note:** This request requires administrator privileges.

**Method:** GET and POST

Syntax:

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=<cmd_type>[&<parameter>=<value>…]

The commands usage and their input arguments are as follows.

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| cmd_type | <string> | Required.<br>Command to be executed, including *search*, *insert*, *delete*, *update*, and *queryStatus*. |

Command: **search**

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| label | <integer primary key> | Optional.<br>The integer primary key column will automatically be assigned a unique integer. |
| triggerType | <text> | Optional.<br>Indicate the event trigger type.<br>Please embrace your input value with single quotes.<br>Ex. mediaType='motion'<br>Support trigger types are product dependent. |
| mediaType | <text> | Optional.<br>Indicate the file media type.<br>Please embrace your input value with single quotes.<br>Ex. mediaType='videoclip'<br>Support trigger types are product dependent. |
| destPath | <text> | Optional.<br>Indicate the file location in camera.<br>Please embrace your input value with single quotes.<br>Ex. destPath ='/mnt/auto/CF/NCMF/abc.mp4' |
| resolution | <text> | Optional.<br>Indicate the media file resolution.<br>Please embrace your input value with single quotes.<br>Ex. resolution='800x600' |
| isLocked | <boolean> | Optional. |

| | | |
|---|---|---|
| | | Indicate if the file is locked or not.<br>0: file is not locked.<br>1: file is locked.<br>A locked file would not be removed from UI or cyclic storage. |
| triggerTime | <text> | Optional.<br>Indicate the event trigger time. (not the file created time)<br>Format is "YYYY-MM-DD HH:MM:SS"<br>Please embrace your input value with single quotes.<br>Ex. triggerTime='2008-01-01 00:00:00'<br>If you want to search for a time period, please apply "TO" operation.<br>Ex. triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59' is to search for records from the start of Jan 1st 2008 to the end of Jan 1st 2008. |
| limit | <positive integer> | Optional.<br>Limit the maximum number of returned search records. |
| offset | <positive integer> | Optional.<br>Specifies how many rows to skip at the beginning of the matched records.<br>Note that the offset keyword is used after limit keyword. |

To increase the flexibility of search command, you may use "OR" connectors for logical "OR" search operations. Moreover, to search for a specific time period, you can use "TO" connector.

Ex. To search records triggered by motion or di or sequential and also triggered between 2008-01-01 00:00:00 and 2008-01-01 23:59:59.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=search&triggerType='motion'+OR+'di'+OR+'seq'&triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59'
```

Command: **delete**

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| label | <integer primary key> | Required.<br>Identify the designated record.<br>Ex. label=1 |

Ex. Delete records whose key numbers are 1, 4, and 8.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=delete&label=1&label=4&label=8
```

Command: **update**

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|

| | | |
|---|---|---|
| label | <integer primary key> | Required.<br>Identify the designated record.<br>Ex. label=1 |
| isLocked | <boolean> | Required.<br>Indicate if the file is locked or not. |

Ex. Update records whose key numbers are 1 and 5 to be locked status.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=1&label=1&label=5
```

Ex. Update records whose key numbers are 2 and 3 to be unlocked status.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=0&label=2&label=3
```

Command: queryStatus

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| retType | xml or javascript | Optional.<br>Ex. retype=javascript<br>The default return message is in XML format. |

Ex. Query local storage status and call for javascript format return message.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=queryStatus&retType=javascript
```

# 8.17 Virtual input (capability.nvi > 0)

**Note:** Change virtual input (manual trigger) status.

Method: GET

Syntax:

```
http://<servername>/cgi-bin/admin/setvi.cgi?vi0=<value>[&vi1=<value>][&vi2=<value>]
[&return=<return page>]
```

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| vi<num> | state[(duration)nstate]<br><br>Where "state" is 0, 1. "0" means inactive or normal state while "1" means active or triggered state.<br>Where "nstate" is next | Ex: vi0=1<br>Setting virtual input 0 to trigger state |
| | | Ex: vi0=0(200)1<br>Setting virtual input 0 to normal state, waiting 200 **milliseconds**, setting it to trigger state.<br>Note that when the virtual input is waiting for next state, |

| | | |
|---|---|---|
| | state after duration. | it cannot accept new requests. |
| return | <return page> | Redirect to the page *<return page>* after the request is completely assigned. The *<return page>* can be a full URL path or relative path according the current path. If you omit this parameter, it will redirect to an empty page. |

| Return Code | Description |
|---|---|
| 200 | The request is successfully executed. |
| 400 | The request cannot be assigned, ex. incorrect parameters.<br>Examples:<br>setvi.cgi?vi0=0(10000)1(15000)0(20000)1<br>No multiple duration.<br>setvi.cgi?vi3=0<br>VI index is out of range.<br>setvi.cgi?vi=1<br>No VI index is specified. |
| 503 | The resource is unavailable, ex. Virtual input is waiting for next state.<br>Examples:<br>setvi.cgi?vi0=0(15000)1<br>setvi.cgi?vi0=1<br>Request 2 will not be accepted during the execution time(15 seconds). |

# 8.18 Open Timeshift Stream (capability.timeshift > 0, timeshift_enable=1, timeshift_c<n>_s<m>_allow=1)

**Note:** This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

```
http://<servername>/<network_http_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&reftime=<value>&forcechk&minsft=<value>]
```

For RTSP (MP4 and H264), the user needs to input the URL below into an RTSP compatible player.

```
rtsp://<servername>/<network_rtsp_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&reftime=<value>&forcechk&minsft=<value>]
```

“n” is the channel index.

"m" is the timeshift stream index.

For details on timeshift stream, please refer to the "TimeshiftCaching" documents.

| PARAMETER | VALUE | DEFAULT | DESCRIPTION |
|---|---|---|---|
| maxsft | <positive interger> | 0 | Request cached stream at most how many seconds ago. |
| tsmode | normal, adaptive | normal | Streaming mode:<br>normal => Full FPS all the time.<br>adaptive => Default send only I-frame for MP4 and H.264, and send 1 FPS for MJPEG. If DI or motion window are triggered, the streaming is changed to send full FPS for 10 seconds.<br>(*Note: this parameter also works on non-timeshift streams.) |
| reftime | mm:ss | The time camera receives the request. | Reference time for maxsft and minsft.<br>(This provides more precise time control to eliminate the inaccuracy due to network latency.)<br>Ex: Request the streaming from 12:20<br>rtsp://10.0.0.1/live.sdp?maxsft=10&reftime=12:30 |
| forcechk | N/A | N/A | Check if the requested stream enables timeshift, feature and if minsft is achievable.<br>If false, return "415 Unsupported Media Type". |
| minsft | <positive interger> | 0 | How many seconds of cached stream client can accept at least.<br>(Used by forcechk) |

| Return Code | Description |
|---|---|
| 400 Bad Request | Request is rejected because some parameter values are illegal. |
| 415 Unsupported Media Type | Returned, if forcechk appears, when minsft is not achievable or the timeshift feature of the target stream is not enabled. |

# 8.19 Export Files

**Note:** This request requires Administrator privileges.

Method: GET

Syntax:

For daylight saving time configuration file:

| |
|---|
| http://<*servername*>/cgi-bin/admin/exportDst.cgi |

For language file:

| |
|---|
| http://<*servername*>/cgi-bin/admin/export_language.cgi?currentlanguage=<value> |

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| currentlanguage | 0~20 | Available language lists.<br>Please refer to:<br>system_info_language_i0 ~ system_info_language_i19. |

For setting backup file:

| |
|---|
| http://<*servername*>/cgi-bin/admin/export_backup.cgi?backup |

# 8.20 Upload Files

**Note:** This request requires Administrator privileges.

Method: POST

Syntax:

For daylight saving time configuration file:

| |
|---|
| http://<*servername*>/cgi-bin/admin/upload_dst.cgi |

Post data:

| |
|---|
| filename =<file name>\r\n<br>\r\n<br><multipart encoded form data> |

For language file:

| |
|---|
| http://<*servername*>/cgi-bin/admin/upload_lan.cgi |

Post data:

| |
|---|
| filename =<file name>\r\n |

| |
|---|
| \r\n<br><multipart encoded form data> |

For setting backup file:

| |
|---|
| http://<*servername*>/cgi-bin/admin/upload_backup.cgi |

Post data:

| |
|---|
| filename =<file name>\r\n<br>\r\n<br><multipart encoded form data> |

Server will accept the file named <file name> to upload this one to camera.

# 8.21 Media on demand

Media on demand allows users to select and receive/watch/listen to metadata/video/audio contents on demand.

**Note:** This request requires Viewer access privileges.

Syntax:

| |
|---|
| rtsp://<servername>/mod.sdp?[&stime=<value>][&etime=<value>][&length =<value>][&loctime =<value>][&file=<value>][&tsmode=<value>] |

| PARAMETER | VALUE | DEFAULT | DESCRIPTION |
|---|---|---|---|
| stime | <YYYYMMDD_HHMMSS.MMM> | N/A | Start time. |
| etime | <YYYYMMDD_HHMMSS.MMM> | N/A | End time. |
| length | <positive integer> | N/A | The length of media of interest.<br>The unit is second. |
| loctime | <boolean> | 0 | Specify if start/end time is local time format.<br>1 for local time, 0 for UTC+0 |
| file | <string> | N/A | The media file to be played. |
| tsmode | <positive integer> | N/A | Timeshift mode, the unit is second. |

Ex.

| stime | etime | length | file | Description |
|---|---|---|---|---|
| V | V | X | X | Play recordings between `stime` and `etime`<br>rtsp://10.10.1.2/mod.sdp?stime=20110312_040400.000<br>&etime=2011_0312_040510.000 |
| V | X | V | X | Play recordings for `length` seconds which start from `stime`<br>rtsp://10.10.1.2/mod.sdp?stime=20110312_040400.000<br>&length=120 |

| | | | | |
|---|---|---|---|---|
| X | V | V | X | Play recordings for `length` seconds which ends at `etime`<br>rtsp://10.10.1.2/mod.sdp?etime=20110312_040400.000&length=120 |
| X | X | X | V | Play file `file`<br>rtsp://10.10.1.2/mod.sdp?filename=/mnt/link0/ |

# 8.22 Remote Camera Control (capability.remotecamctrl.master>0)

**Note:** This request requires Viewer access privileges.

Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/camctrl/rCamCtrl.cgi?[channel=<value>]
[&x=<value>&y=<value>&r=<value>&videosize=<value>&resolution=<value>&stretch=<value>] – Click on image
[&camid=<value>]
[&return=<return page>]

Example:

http://myserver/cgi-bin/camctrl/rCamCtrl.cgi?channel=0&x=300&y=200&r=100&resolution=1920x1920&videosize=1920x1920&strech=1&camid=0

| PARAMETER | VALUE | DESCRIPTION |
|---|---|---|
| channel | <0~(n-1)> | Channel of video source. |
| x | <integer> | x-coordinate clicked by user.<br>It will be the x-coordinate of client side camera after movement. |
| y | <integer> | y-coordinate clicked by user.<br>It will be the y-coordinate of client side camera after movement. |
| r | <integer> | radius select by user. It will be the roi view area radius of client side camera after movement and zooming. |
| videosize | <window size> | The size of plug-in (ActiveX) window in web page |
| resolution | <window size> | The resolution of streaming. |
| stretch | <boolean> | 0 indicates that it uses **resolution** (streaming size) as the range of the coordinate system.<br>1 indicates that it uses **videosize** (plug-in size) as the range of the coordinate system. |
| camid | 0,<positive integer> | slave camera ID |

| | | |
|---|---|---|
| return | <return page> | Redirect to the page *<return page>* after the parameter is assigned. The *<return page>* can be a full URL path or relative path according to the current path. If you omit this parameter, it will redirect to an empty page. |

**Return code:** clickimg_return="$Error_code"

| Error code | Code - Hexa | Code - Decimal | Description | SysLog message |
|---|---|---|---|---|
| CLICKIMG_SUCCESS | 0x000000C8 | 200 | Success to control auxiliary camera | |
| ERR_CONNECTION | 0x000001F4 | 500 | Controller camera connect to auxiliary camera fail. | PPTZ_Connection fail |
| ERR_UNSUPPORT_POS | 0x000001F5 | 501 | Controller camera can't get the correspond position from mapping table. | PPTZ_Unsupported position |
| ERR_MODULE_DISABLE | 0x000001F6 | 502 | Panoramic PTZ function is disable | PPTZ_Function is disabled |
| ERR_INVALID_CAM_ID | 0x000001F7 | 503 | Invalid auxiliary camera id. | PPTZ_Invalid auxiliary camera ID |
| ERR_INVALID_FORMAT | 0x000001F8 | 504 | Invalid CGI command, if you lost any one of the required parameter, it will cause fail. | PPTZ_Invalid cgi command format |

# 8.23 Upload map file (capability.remotecamctrl.master>0)

**Note:** This request requires Admin privileges.

Method: POST

Syntax:

http://<*servername*>/cgi-bin/admin/upload_map.cgi?camid=<value>

– Upload map file

Return code

- Upload fail:

upload_result=1

upload_msg=<value>

- Upload success:

upload_result=0

upload_msg=<value>

[ip=<value>] , not exist in map file: default ip = ""

[port=<value>] , not exist in map file: default port = 80

[username=<value>] , not exist in map file : default username = ""

[passwd=<value>] , not exist in map file : default passwd = ""

# 8.24 Export map file (capability.remotecamctrl.master>0)

**Note:** This request requires Admin privileges.

Method: GET

Syntax:

http://<*servername*>/cgi-bin/admin/export_map.cgi?camid=<value>

– Export map file

<End of document>

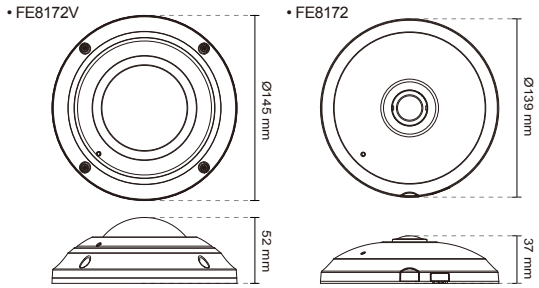
# Technical Specifications

## Technical Specifications

| | |
|---|---|
| Models | SF8172<br>SF8172V (Vandal-proof) |
| **System Information** | |
| CPU | Multimedia SoC (System-on-Chip) |
| Flash | 128 MB |
| RAM | 128 MB |
| **Camera Features** | |
| Image Sensor | 1/2.5" Progressive CMOS in 2560x1920 resolution |
| Maximum Resolution | 1920x1920 |
| Lens Type | Fixed-focal |
| Focal Length | f = 1.05 mm |
| Aperture | F2.8 |
| Field of View | 180° (horizontal)<br>180° (vertical)<br>180° (diagonal) |
| Shutter Time | 1/5 sec. to 1/32,000 sec. |
| WDR Technology | WDR Enhanced |
| Day/Night | Removable IR-cut filter for day & night function |
| Minimum Illumination | 0.03 Lux @ F2.8, 50 IRE (Color)<br>0.001 Lux @ F2.8, 50 IRE (B/W) |
| Pan/tilt/zoom Functionalities | ePTZ:<br>12x digital zoom (12x on IE plug-in) |
| On-board Storage | MicroSD/SDHC/SDXC card slot |
| **Video** | |
| Compression | H.264, MJPEG & MPEG-4 |
| Maximum Frame Rate | H.264:<br>15 fps at 1920x1920<br>30 fps at 1920x1080<br>MPEG-4:<br>15 fps at 1920x1920<br>30 fps at 1920x1080<br>MJPEG:<br>15 fps at 1920x1920<br>30 fps at 1920x1080 |
| Maximum Streams | 3 simultaneous streams |
| S/N Ratio | Above 62 dB |
| Dynamic Range | 57 dB |
| Video Streaming | Adjustable resolution, quality and bitrate |
| Image Settings | Adjustable image size, quality and bit rate<br>Pixel counter<br>Time stamp, text overlay, flip & mirror<br>Configurable brightness, contrast, saturation, sharpness, white balance, exposure control, gain, backlight compensation, privacy masks<br>Scheduled profile settings |
| **Audio** | |
| Audio Capability | Audio input/output (full duplex) |
| Compression | GSM-AMR, AAC, G.711 |
| Interface | Built-in microphone<br>External microphone input |
| Effective Range | 5 meters |
| **Network** | |
| Users | Live viewing for up to 10 clients |
| Protocols | IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTCP, IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, CoS, QoS, SNMP, 802.1X |
| Interface | 10Base-T/100 BaseTX Ethernet (RJ-45) |
| ONVIF | Supported, specification available at www.onvif.org |
| **Intelligent Video** | |
| Video Motion Detection | Five-window video motion detection |

| | |
|---|---|
| **Alarm and Event** | |
| Alarm Triggers | Video motion detection, manual trigger, digital input, periodical trigger, system boot, recording notification, camera tampering detection |
| Alarm Events | Event notification using digital output, HTTP, SMTP, FTP and NAS server<br>File upload via HTTP, SMTP, FTP and NAS server |
| **General** | |
| Connectors | RJ-45 cable connector for Network/PoE connection<br>Audio input<br>Audio output<br>12V DC power input<br>Digital input*1<br>Digital output*1 |
| LED Indicator | System power and status indicator |
| Power Input | 12V DC<br>IEEE 802.3af PoE Class 2 |
| Power Consumption | Max. 5.1 W (12V DC)<br>Max 5.3 W (PoE) |
| Dimensions | Ø: 145 mm x 52 mm (SF8172V)<br>Ø: 139 mm x 37 mm (SF8172) |
| Weight | Net: 545g (SF8172V)<br>Net: 358g (SF8172) |
| Casing | Vandal-proof IK10-rated metal housing (SF8172V)<br>Weather-proof IP66-rated housing (SF8172V) |
| Safety Certifications | CE, LVD, FCC Class A, VCCI, C-Tick, UL<br>EN50155 (SF8172V) |
| Operating Temperature | Starting Temperature: -25°C ~ 50°C (-13°F ~ 122°F)<br>Working Temperature: -40°C ~ 50°C (-40°F ~ 122°F) |
| Warranty | 36 months |
| **System Requirements** | |
| Operating System | Microsoft Windows 7/Vista/XP/2000 |
| Web Browser | Mozilla Firefox 7~10 (Streaming only)<br>Internet Explorer 7.x or 8.x |
| Other Players | VLC: 1.1.11 or above<br>QuickTime: 7 or above |
| **Included Accessories** | |
| CD | User's manual, quick installation guide, Installation Wizard 2, VAST CMS (90-day free trial version) |
| Others | Quick installation guide, warranty card, alignment sticker, desiccant bag, screw driver, screws pack, I/O cable, mounting bracket |

## Dimensions




## Compatible Accessories

Mounting Kits

*Ceiling Mount:*


**AM-51A**
Dome adapter


**AM-517**
NPT adapter


**AM-114**
Pendant head


**AM-117**
Pendant pipe (40 cm)

*Wall Mount:*


**AM-51A**
Dome adapter


**AM-517**
NPT adapter


**AM-116**
Pendant pipe (20 cm)


**AM-212**
Wall mount bracket

Power Adapter


**AA-221**
12V DC Power Adapter

PoE Kits


**POE-IJ-1748NDN**
PoE injector, 802.3af compliant

# Technology License Notice

## MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT WITH REGARD TO PC SOFTWARE, OF WHICH YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO HTTP://WWW.VIALICENSING.COM.

## MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. PLEASE REFER TO HTTP://WWW.MPEGLA.COM.

## AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

# Electromagnetic Compatibility (EMC)

## FCC Statement

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

## CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

## VCCI Warning

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準にづくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい

## Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.